13th ICCRTS: C2 for Complex Endeavors

“Networking the Global Maritime Partnership”

Mr. George Galdorisi
SPAWAR Systems Center San Diego

Dr. Stephanie Hszieh
SPAWAR Systems Center San Diego

Mr. Terry McKearney
The Ranger Group

Point of Contact:

Stephanie Hszieh

SPAWAR Systems Center San Diego

53560 Hull Street
Code 73500
San Diego CA 92152-5001

(619) 553-4817

hszieh@spawar.navy.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
JUN 2008

2. REPORT TYPE

3. DATES COVERED
00-00-2008 to 00-00-2008

4. TITLE AND SUBTITLE
Networking the Global Maritime Partnership

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SPAWAR Systems Center San Diego,Code 73500,53560 Hull Street,San Diego,CA,92152-5001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA

14. ABSTRACT

The modern-day notion of a ?Global Maritime Partnership,? first introduced by then-CNO Admiral Michael Mullen at the 2005 International Seapower Symposium as ?The 1000-Ship Navy,? and later enshrined in the new U.S. Maritime Strategy, A Cooperative Strategy for 21st Century Seapower, is rapidly gaining worldwide currency as many nations and navies seek to work together to combat global terrorism?as well as a host of other issues?in the maritime arena. But neither networking nor global maritime partnerships are new concepts and understanding the history of naval coalition operations and of networking in the maritime environment can help nations and navies understand the challenges to fielding an effective global maritime partnership in the 21st Century. Armed with this historical perspective, coalitions can begin to devise effective solutions to these challenges. One of the biggest challenges to instantiating an effective global maritime partnership is technical?how do the navies of disparate nations that desire to operate together at sea obtain the requisite, compatible C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) systems that will enable them to truly ?network? and make the global maritime partnership a reality. Unless or until the technical challenges to networking navies at sea are addressed by the U.S. Navy and by likely coalition navies, the dream of a global maritime partnership will never be achieved.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**78**	

Networking the Global Maritime Partnership

Abstract

The modern-day notion of a "Global Maritime Partnership," first introduced by then-CNO Admiral Michael Mullen at the 2005 International Seapower Symposium as "The 1000-Ship Navy," and later enshrined in the new U.S. Maritime Strategy, *A Cooperative Strategy for 21st Century Seapower*, is rapidly gaining worldwide currency as many nations and navies seek to work together to combat global terrorism—as well as a host of other issues—in the maritime arena.

But neither networking nor global maritime partnerships are new concepts and understanding the history of naval coalition operations and of networking in the maritime environment can help nations and navies understand the challenges to fielding an effective global maritime partnership in the 21st Century. Armed with this historical perspective, coalitions can begin to devise effective solutions to these challenges.

One of the biggest challenges to instantiating an effective global maritime partnership is technical—how do the navies of disparate nations that desire to operate together at sea obtain the requisite, compatible C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) systems that will enable them to truly "network" and make the global maritime partnership a reality. Unless or until the technical challenges to networking navies at sea are addressed by the U.S. Navy and by likely coalition navies, the dream of a global maritime partnership will never be achieved.

Keywords: Global Maritime Partnership, 1000-Ship Navy, networking, FORCEnet, C4ISR, The Technical Cooperation Program (TTCP)

Background

The United States' new maritime strategy, titled *A Cooperative Strategy for 21st Century Seapower* has made cooperation a key element in the future of U.S. Navy operations. The new strategy looks at cooperation at two levels—cooperation at home and cooperation abroad. Cooperation at home included the fact that this new strategy was signed by the leaders of the US's three primary maritime forces—Navy, Marine Corps, and Coast Guard. Cooperation abroad is seen in the concept of the global maritime partnership that calls for the formation of an informal network of maritime forces dedicated to maintaining the safety and security of the world's oceans and sea lanes.

The present-day concept of a global maritime partnership can be traced back to Admiral Michael Mullen's tenure as U.S. Navy Chief of Naval Operations. His original concept of "The 1000-Ship Navy"—a global navy composed of 1000 or more ships working cooperatively—evolved into the Global Maritime Partnership. Admiral Mullen introduced the concept at the 2005 International Seapower Symposium in Newport, Rhode Island, stating:

> "As we combine our advantages, I envision a thousand-ship navy—a fleet-in-being, if you will—made up of the best capabilities of all freedom-loving navies of the world… This thousand-ship navy would integrate the capabilities of the maritime services to create a fully interoperable force, an international city at sea." [1]

Subsequent to this initial unveiling of the concept, U.S. Navy representatives, including the CNO himself, extolled the virtues of a global maritime partnership at national and international security conferences and articles about the global maritime partnership began to appear in national and international professional journals.[2] Concurrently, other nations and navies embraced this concept along with the general recognition that globalization required a concerted team effort to police the maritime commons and that no single nation could do it alone.

The U.S. Navy's new maritime strategy that was unveiled at the 2007 International Seapower Symposium (ISS) in Newport, Rhode Island notes, "No one nation has the resources required to provide safety and security throughout the entire maritime domain."[3] These words aptly summarize the core intent of the U.S. Navy's *A Cooperative Strategy for 21st Century Seapower*—to encourage and sustain a global maritime partnership of the world's navies to maintain the freedom and security of the seas. The new maritime strategy's unveiling in front of an audience of over 100 representatives of international navies and coast guards emphasized the theme of international cooperation on the high seas.[4]

Subsequent to the publication of *A Cooperative Strategy for 21st Century Seapower*, U.S. Navy officials pointed out that the U.S. Navy does not intend to lead this global maritime partnership but will be a willing partner with other nations and navies—especially regional navies—operating on the global commons to defeat international terrorism.[5] As Admiral Roughead noted at the 2007 ISS, "The key to all of this is trust. We believe that trust is something that cannot be surged. Trust is something that must be built over time."[6]

With the international groundswell the United States created in promoting the value of a global maritime partnership, expectations are high that the U.S. Navy will be an important contributor to this effort and U.S. Navy ships will be able to operate effectively with likely coalition partner navies on the global commons. This expectation has also created the assumption that the U.S. Navy will be able to network effectively with navies that have disparate—often widely disparate—C4ISR capabilities.

But the technical challenges to networking navies at sea are not trivial, and absent significant technical work by all navies involved to fashion compatible C4ISR systems—with the U.S. Navy a major contributing partner—the dream of a global maritime partnership will never be achieved. The ideas of "networking at sea" and "global maritime partnerships" are not new. Understanding some of the history—and challenges—that navies have dealt with in the past can help provide a road ahead for a truly networked global maritime partnership.

Perspective: Coalitions, Networking, and Technology

Some believe that networking—especially at sea—was a brand new concept first introduced by the late Vice Admiral Arthur Cebrowski and John Gartska in the January 1998 *U.S. Naval Institute Proceedings*.[7] Similarly, some also believe the concept of a global maritime partnership was unknown until it was unveiled by Admiral Mullen and subsequently featured in the November 2005 *U.S. Naval Institute Proceedings* in an article by Vice Admiral John Morgan and Rear Admiral Charles Martoglio.[8] Nothing could be further from the truth and understanding this rich history is instrumental in coming to grips with some of the challenges of a 21st Century global maritime partnership.

Coalition Naval Operations

Maritime coalitions have existed for two and one-half millennia and navies have communicated at sea for at least that long. As far back as the Greco-Persian War (499 B.C. – 449 B.C.) naval coalitions have come together—often on a short-notice, ad hoc basis—in the same way that the U.S. Navy envisions today's global maritime partnership operating.[9] Two millennia ago—and even through the 16th Century, these naval coalitions communicated in fairly rudimentary ways—from shouts of command from ship-to-ship to the lighting of signal fires on board to signal the start of action.[10]

Maritime coalitions changed over time and technology often aided navies seeking to operate together. The invention of the telescope and binoculars in the early 1600s facilitated the ability of ships to communicate with each other at a greater distance.[11] The primary means of communications were signal flags that were used to convey simple instructions and warnings to the fleet. In addition to signal flags, cannon fire, lanterns, and messages sent by small boats between ships were also used to communicate commands or information.[12] While "signal books" were proprietary to each navy, those navies could usually arrive at agreed-to principals to communicate.[13]

The end of the 19th Century ships saw the beginning of more complex naval maneuvers as technological breakthroughs such as the application of the steam engine, the iron hull, and electronic communications to naval warfare enabled armadas of ships to literally circle the globe.[14] In the days before the advent of electronic communications, naval communications between ship and shore and between ships typically took weeks or months.

> "…the United States Navy's Pacific Squadron had to communicate with the Navy Department in Washington by dispatch vessel sailing round Cape Horn…Consequently in 1846 they did not know of an outbreak of

> war with Mexico until an officer traveling overland managed to get a message through privately."[15]

The speed-up of communications due to the electronic telegraph allowed naval commanders to keep better track of their forces and ongoing events around the world.[16] With fleets able to operate further way from their commands and commanders able to keep informed though new communication technologies powered by electricity, the need to communicate at sea—something navies that partnered together could do somewhat effectively—morphed into the need to *network* at sea. This presented navies with new challenges as the technological bar was raised.

Networking at Sea

Networking at sea—the ability of naval commanders to have a cooperatively-created tactical picture—had long been the dream of naval commanders who wanted to be able to see what was over the horizon.[17] The dawn of the 20th Century saw the evolution of technologies that held the potential to at least begin some rudimentary networking at sea.

In 1904, Britain's First Sea Lord, Admiral John Fisher, took advantage of the new technology and developed what Dr. Norman Friedman has dubbed "picture-based" warfare.[18] Admiral Fisher used the information gleaned from shipping reports and reports from his own fleets to build a tactical picture of where pirates were attacking British merchant ships. Information from these sources was fed into two different war rooms—the first war room tracked ship movements around the world while the second war room tracked ship movements in the North Sea. Armed with this "picture-based" view of the world, Admiral Fisher was able to direct warships to the spots where pirates were attacking British ships.

As technology evolved, so did the ability of navies to use this new concept of "networking" to achieve decisive results. In World War II British convoys and U.S. aircraft formed a successful intelligence-based network to defeat German U-Boat attacks.[19] During the Cold War, the U.S.—often in concert with coalition partners such as Great Britain and Canada—networked information obtained by sound surveillance systems (SOSUS) with ASW aircraft to track Soviet submarines. For the U.S. Navy, this ultimately evolved in the 1990s to the Copernicus C4I initiative primarily designed to create a common tactical picture.[20] The Joint On-line Tactical System (JOTS), implemented in the Mediterranean Sea during the late 1980s, was an early attempt to network across the Services. JOTS utilized U.S. Navy and U.S. Air Force intelligence and sensor networks to build shared situational awareness for the component commanders.[21]

Technology and Technological Challenges

As nations, and especially navies, adopted new technologies, they found that often the technological promise of a new system was accompanied by unintended consequences that sometimes made the net result a negative rather than a positive. For example, the introduction of the telegraph promised instantaneous communications across vast distances. No longer would messages take months to traverse continents as telegraph cables and networks made it possible for messages to be relayed in days. The Royal Navy found the telegraph to be an important tool in communicating with its global fleet, but that ease and speed of communications came with a price. During times of tension, fleet commanders were often found on their command ship docked at port in order to have access to telegraph messages rather than out at sea with their ships.[22]

But the telegraph, a breakthrough technology that all assumed would “cure” a universe of communications ills had another downside—an “unintended consequence” of its use.[23] Prior to the invention of the telegraph British expatriates at the far end of the empire received news of events transpiring in the British Isles through bundles of newspapers delivered by ship. This typically took anywhere from four to six weeks but when the news arrived it was robust, detailed and provided the reader with virtually all they could have wanted to know about these events—absent being there in person.

The Victorians eagerly embraced the telegraph as something that was “faster and better” that would provide them the “news of the home islands” instantly and without the multi-week time delay. But this new technology had a downside. Telegraph transmissions were expensive so those putting together telegraph messages put a premium on brevity and “news” was truncated to the bare essentials. Additionally, transmissions were sent from one way station to the next where one operator had to manually key in what he or she had just received, a process that was fraught with error—and was doubly chancy since not all operators at these way stations spoke English. The net result was that when the news finally arrived it was truncated, error-prone and often bore little resemblance to the initial information that was transmitted.[24]

The advent of wireless technology also brought the promise of better and speedier communications between command and fleets at sea. Navies were no longer bound by land-locked telegraph cables and signals could reach out into the vast expanse of the sea allowing for central command to better track their forces. This centralized control allowed for better vectoring of fleets based on a centralized information system, but also made it harder for fleet commanders to manage their ships. Professor N.A.M. Rodger of the University of Exeter tells of an incident in 1942 when the commander of the Royal Navy’s Home Fleet, Admiral John Tovey, asked the Admiralty to take command of his ships as he had lost track of them while at sea.[25]

And not unlike the telegraph, wireless had another “unintended consequence.” While wireless technology helped commanders reach far-flung units and communicate in real time, *enemy* units could also copy these same transmissions for their tactical advantage. History is replete with examples of navies and other forces suffering defeat because the enemy intercepted wireless communications.

Naval forces today, particularly the U.S. Navy, have embraced current communication technologies like the Internet and satellite communications to maintain situational awareness and track its global fleet. However, much like the Royal Navy in the days of the telegraph and wireless communications, the U.S. Navy must today deal with the challenges posed by these new technologies. The Navy's networking effort is through the overarching functional concept called FORCEnet that ties all naval C4ISR to the larger defense Global Information Grid (GIG).[26] The challenge now is how can the Navy ensure that its multi-billion dollar initiative to fully network the fleet *enhances* U.S. Navy participation in the global maritime partnership rather than impedes partnership activities. As the U.S. Navy is surging forward in building a modern force with advance information technologies, is it creating an unintended consequence by leaving coalition partner navies in its wake?

Naval Coalition Networking: How Big a Problem?

For the U.S. Navy, there is a strong desire to effectively network at sea. Writing in the capstone publication of the OSD Office of Force Transformation, Vice Admiral Arthur Cebrowski noted, "The United States wants its partners to be as interoperable as possible. Not being interoperable means you are not on the net, so you are not in a position to derive power from the information age."[27]

Unfortunately, that "want" is not being realized today. Each year, the five numbered fleet commanders in the U.S. Navy submit their "top ten C4ISR requirements." For years, these "desirements" have been literally all over the map, with "more bandwidth" often taking top billing. Today, these fleet commanders all identify one C4ISR issue as their top priority—coalition communications.[28] These warfighters recognize that the ability to communicate and exchange data with coalition partners is important to their success across a wide range of mission areas, but also that networking with the coalition partners in their areas of responsibility is increasingly challenging.

The imperative to provide the Navy's operational commanders with better tools for coalition communications has percolated to the highest levels of the Department of the Navy. Soon after assuming his duties as Deputy Chief of Naval Operations for Communications Networks, Vice Admiral Mark Edwards stressed the crucial importance of networking coalition partners. In a memorandum to the Director of the Warfare Integration Division entitled "FORCEnet for the 1000-Ship Navy," Vice Admiral Edwards directed his staff to:

> "Lead an effort to articulate the strategy to network the 1000-Ship Navy… identify the funding, personnel, organization, and processes for ensuring interoperability with coalition navies at the sensitive but unclassified level where possible…ensure coalition interoperability is considered at the earliest stages of capability development."[29]

The Assistant Secretary of Defense for Networks and Information Integration (ASD NII)—the highest authority on C4ISR in the U.S. military—has recognized both the importance of coalition networking and the challenges of its implementation. Dr. David Alberts, Director of Research for the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII), explained this dilemma at a high-level symposia noting, “In today’s world, nothing significant can get done outside of a coalition context,” while also noting, “We have been *humbled* by the challenges of devising effective coalition communications.”[30]

Though daunting as it may be to establish effective coalition communications, there is a growing body of information that shows that it is possible and has dramatic benefits. One example of this occurred during the 1999 air operations in Kosovo that required extensive coalition interoperability between allied air forces. During the operation, which resulted in over 36,000 sorties flown to support the peacekeeping mission, it was discovered that the allied air force command had trouble tracking, locating, and fixing mobile targets on the ground.[31] Weather and terrain were inhibiting pilots and forward air controllers from detecting mobile targets. The solution to the problem was to network sensors, analysts, decision makers, and pilots together into a global kill chain. Networking allowed information obtained by Predator Unmanned Aerial Vehicles (UAV) to be shared by all in the kill chain to increase the detection of those troublesome mobile targets.[32] Examples like this are growing but there remains a much larger challenge that is emerging as coalition operations increase to include non-traditional coalition partners and nations with differing rates of modernization.[33]

The challenges for the U.S. Navy as it attempts to network with coalition partners is gaining increased world-wide recognition. Writing in the authoritative *Naval War College Review*, Professor Paul Mitchell, the former Director of Academics at the Canadian Forces College, asked the key question:

> “Is there a place for small navies in network-centric warfare? Will they be able to make any sort of contribution in multinational naval operations of the future? Or will they be relegated to the sidelines, undertaking the most menial of tasks, encouraged to stay out of the way—or stay at home…The ‘need for speed’ in network-centric operations places the whole notion of multinational operations at risk.”[34]

From the perspective of potential coalition partners there are two technological challenges that impact efforts to effectively network with the United States Navy. The first is purely technological. Potential partnering navies, even the most sophisticated ones, do not generally have comparable installed networking capability aboard their ships and aircraft. While many have U.S. Navy systems such as Link 11, there is limited availability of Internet Protocol (IP) bandwidth aboard most of our coalition partners’ ships. The increasing sophistication of collaboration for the newer missions coalition forces are undertaking relies on the technologies based on IP connectivity: email, chat, FTP file sharing, and video teleconferencing. Without access to this capability, coalition ships find themselves unable to fully participate in force-wide planning activities undertaken by U.S. Navy commanders. Providing extended IP services to coalition ships operating as part of the global maritime partnership is a persistent issue in building a coalition networking capability.

A second challenge potential partners face in integrating networking efforts with the US Navy is rooted in the respective procurement policies the U.S. Navy and these partners are bounded by. The US Navy's "POM" (Program Objective Memorandum) process for budgeting follows a long range path to procuring new technologies with supporting research and development effort tied to this "long range" view. This process serves the US Navy's needs to do large scale procurements for many ships with an eye towards increasingly sophisticated capabilities. Conversely, most of the US Navy's potential coalition partners face more restrictive budgets in a procurement process that favors limited procurement in a shorter cycle. In practical terms this often results in these potential partners advocating a "good enough" technology solution now as opposed to an ostensibly better one in the future.

Efforts are currently underway at the technical grass roots level to provide solutions to networking between partner navies. One example is the development of the Combined Enterprise Regional Information Exchange System (CENTRIXS)—a global information-sharing network established in 2002.[35] CENTRIXS has been used by the U.S. Navy and partner nations to network across the maritime domain in coalition efforts like Operation Enduring Freedom. While CENTRIXS has helped to solve current networking issues, there remains a need for more permanent, long-term efforts to deal with issues like building a network that can sustain the massive data rates that will be needed to truly network in the future.[36]

Successive U.S. Navy Chiefs of Naval Operations have extolled the virtues of coalition naval operations, but have also emphasized that the U.S. Navy will not slow down technologically to allow other navies to catch up. While naval planners and policy makers continue to discuss the importance of coalition networking, the U.S. Navy still needs to acknowledge the substantial policy, doctrinal and, increasingly, technical challenges to effectively network the global maritime partnership.

Part of the challenge for the Navy is that coalition interoperability does not fit neatly into any requirements "bin" for the U.S. Navy or for the navies of other major maritime powers. It does not fly, float, or operate beneath the seas. It does not strike the enemy from afar like cruise missiles. It does not enhance readiness like spare parts or training. Thus, it often does not always have the requisite degree of high-level advocacy. This is not to imply that those in charge of setting requirements or acquiring weapons systems are not keen on doing the right thing—clearly they are. The challenge to fit coalition communications into the requirements and acquisition process is that it takes a great deal of time and attention to change the process and practices that have grown up over the decades. As yet, it is a journey that is incomplete.

But is there a "way forward" for the U.S. Navy in its quest for a means to network effectively as part of the global maritime partnership? Is there a "best practices" model that can provide a compelling demonstration of the value of effective coalition networking? The answer to these two questions is "yes," and it is an example that must be extrapolated to additional likely coalition partner navies as a *necessary condition* for achieving the global maritime partnership.

A Way Forward?

For the U.S. Navy, the technical challenges to effectively network with likely coalition partners are not trivial. Specifically, for a 21st Century FORCEnet-centric U.S. Navy, the challenge is twofold: quantifying the operational effectiveness of a coalition force networked via the U.S. Navy infrastructure provided by FORCEnet, versus the operational effectiveness of a coalition force less-robustly networked, and finding a way for likely coalition partners to co-evolve maritime networking systems in a way that enables maximum networking among partner ships and other platforms.[37]

The issue of co-evolution is an important one because for a U.S. Navy determined to be a global maritime *partner*, and not a naval power that dominates partners with U.S.-centric solutions, a cooperative arrangement regarding technology development is crucial.[38] And this implies early and frequent cooperation and collaboration at the grass roots level by scientists and engineers working in laboratories of global maritime partners to come up with technical solutions for challenging networking problems.

Bringing coalition naval ships and aircraft together on the global maritime commons is challenging enough, and it would appear to be dwarfed by the challenge of bringing scientists and engineers at coalition-partner national laboratories together to address common challenges. But such a model does exist under the auspices of The Technical Cooperation Program (TTCP).

TTCP is a forum for defense science and technology collaboration between Australia, Canada, New Zealand, the United Kingdom, and the United States. It was formed in 1957 as the Tripartite Technical Cooperation Program and has grown into an extensive international collaborative defense science and technology activity.[39] The aim of TTCP is to foster cooperation within the science and technology areas needed for national defense. To do this, TTCP provides a formal framework that scientists and technologists can use to share information with one another.

For the past six years one TTCP Group, the Maritime Systems Group, has been working on the topics of "Networking Maritime Coalitions," and "FORCEnet and Coalition Implications." The group has generated analytical data and conducted modeling and simulation to demonstrate that if the U.S. Navy's FORCEnet is developed in a way that is inclusive of likely coalition partners, who, in turn, build their national systems to be compatible with FORCEnet, the naval forces involved will enjoy a quantum increase in capability.

The Maritimes Systems Group has now begun the important effort of informing national naval C4ISR acquisition programs so that the five participating nations can co-evolve their systems in a way that will enable them to seamlessly network at sea. This includes identifying "technology on-ramps" within the acquisition commands of each nation where the right systems can be procured and subsequently installed on each nation's ships at the right time in order to "grow" compatible C4ISR systems in concert.

Although TTCP focuses on addressing technological issues that arise in developing military coalitions, the Maritime System Group's efforts have allowed the participating nations' navies to address issues rooted in the strategic and tactical priorities of these navies themselves. In terms of coalition force building, it is obvious that coalition partners would bring different and varied capabilities to the force based on these individual priorities. The Maritime System Group's modeling and analysis efforts have allowed individual nations to emphasize respective capabilities and operational objectives in their modeling, allowing them the ability to explore the impact of networking on these individual priorities and, in turn, articulate the impact of these priorities on a coalition force. This has enriched the group's understanding of the tactical capabilities of each of the partners and led to a more sophisticated understanding of the practical challenges in guiding coalition naval forces in a variety of missions. It has also led to a greater understanding of each nation's issues and concerns in developing naval capabilities.

But TTCP represents just five nations, and as good as the group's work products might be, the circle of influence of these products is limited to just five nations. For the envisioned global maritime partnership to succeed, a variety of navies capable of operating together on short notice and across a spectrum of missions is required, and similar analytical work will need to be undertaken, and soon, in other venues. NATO offers one potential forum that would include a large number of navies. ASEAN and the nations in the U.S. Southern Command AOR represent other groups of nations that would likely work together across a wide spectrum and that would benefit from enhanced communications and networking at sea.

However, the TTCP model provides a means for the laboratory communities in the nations that will likely work together at sea to analyze technical communication and networking needs in an operational framework. And the importance of doing this work at the laboratory level cannot be overstated. The current U.S. SOUTHCOM commander highlighted this in an article in the *U.S. Naval Institute Proceedings* when he stated: "We will win—or lose—the next series of wars in our nation's laboratories."[40] The application of the TTCP model of collaboration between national laboratories of partner nations to current and future efforts to build effective coalition communication networks can be an important step in realizing the goals of the global maritime partnership.

Conclusion: Challenge and Opportunity

The groundswell of enthusiasm among nations that share a common strategic objective to forge an effective global maritime partnership is palpable. But the hard technical work—at the laboratory level—needs to begin *now*. This is because naval leaders will not be convinced to provide the resources to enable this networking at sea unless they see the rigorous analytical underpinning that conclusively demonstrates the enhanced operational effectiveness that one navy gains by networking with its coalition partners. And absent the requisite technology infusion within *all* of these navies, the dream of empowering commanders at the edge will not be realized.

[1] "A Global Network of Nations for a Free and Secure Maritime Commons," *Report of the Proceedings of the 17th International Seapower Symposium*, 19-23 September 2005, <http://www.nwc.navy.mil/cnws/marstrat/docs/library/ISS17web.pdf >.

[2] See, for example, remarks by U. S. Chief of Naval Operations, Admiral Michael Mullen, at the Royal United Services Institute for Defence and Security Studies Future Maritime Warfare Conference, London, United Kingdom, 13 December 2005, accessed at: www.rusi.org; George Galdorisi and Darren Sutton, "Achieving the Global Maritime Partnership: Operational Needs and Tactical Realities," *RUSI Defence Systems*, 15 June 2007; Vice Admiral John Morgan, USN, "A Navy of Navies," *RUSI Defence Systems*, summer 2006, pp. 66-68; and Vice Admiral J. Morgan and Rear Admiral C. Martoglio, "The 1000-Ship Navy: Global Maritime Network," *United States Naval Institute Proceedings*, November 2005, pp. 14-17.

[3] *A Cooperative Strategy for 21st Century Seapower* (Washington, D.C.: Department of the Navy, 2007). Accessed on the Department of the Navy website at www.navy.mil.

[4] Jennifer Grogan, "Seapower Symposium Focuses on Post-Cold War Challenges," *New London Day*, 18 October 2007.

[5] Ronald E. Ratcliff, "Building Partners' Capacity: The Thousand-Ship Navy," *Naval War College Review*, Autumn 2007, pp. 46-49. For examples of this ad-hoc maritime coalition at work see Geoffrey Till, "New Directions in Maritime Strategy? Implications for the U.S. Navy," *Naval War College Review*, autumn 2007, p. 36.

[6] Jim Garamone, "Sea Services Unveil New Maritime Strategy," *American Forces Press Service*, 17 October 2007. See also, Grogan, "Seapower Symposium."

[7] See Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *United States Naval Institute Proceedings*, January 1998, pp. 28-35. See also the following for more information about network centric warfare: David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C: Command and Control Research Program, 1999); David S. Alberts, John J. Garstka, Richard E. Hayes, and David t. Signori, *Understanding Information Age Warfare* (Washington, D.C.: Command and Control Research Program, 2001); David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, D.C.: Command and Control Research Program, 2003); and David S. Alberts and Richard E. Hayes, *Understanding Command and Control* (Washington, D.C.: Command and Control Research Program, 2006).

[8] Vice Admiral Morgan and Rear Admiral Martoglio, "The 1000 Ship Navy," pp. 14-17.

[9] G.P. Gilbert and Lieutenant A. Argirides, "C3I in the Persian and Greek Fleets – 499 to 431 BCE: When the *King of Kings* and the *Nauarchos* Ruled the Waves," paper presented at the 2007 Royal Australian Navy King Hall Naval History Conference, Sydney/Canberra, Australia, 26-27 July 2007.

[10] William Ledyard Rodgers, *Greek and Roman Naval Warfare: A Study of Strategy, Tactics, and Ship Design from Salamis (480 B.C.) to Actium (31 B.C.)* (Annapolis, MD: United States Naval Institute Press, 1964), p. 106.

[11] Linwood S. Howeth, *History of Communications-Electronics in the United States Navy* (Washington, D.C.: Bureau of Ships and Office of Naval History, 1963), p. 4.

[12] Brian Tunstall, *Naval Warfare in the Age of Sail: The Evolution of Fighting Tactics 1650-1815* (London: Conway Maritime Press Limited, 1990), pp. 8-9.

[13] Timothy Wilson, *Flags at Sea* (Annapolis, MD: Naval Institute Press, 1986), p. 77. The British Royal Navy's 100 years of experimentation with common signal books (a.k.a. instructions) is a prime example of naval efforts to better communicate with each other.

[14] H.P. Willmott, *Sea Warfare: Weapons, Tactics and Strategy* (Strettington, England: Antony Bird Publication, 1981), p. 27 and also E.B. Potter, ed., *Sea Power: A Naval History*, 2nd ed. (Annapolis, MD: Naval Institute Press, 1981), p. 109.

[15] Arthur Hezlet, *Electronics and Sea Power* (New York: Stein and Day, 1975), p. 3.

[16] Howeth wrote of the U.S. Navy's experience with the electric telegraph: "By 1890 commercial telegraphic or cable facilities were available in practically every port frequented by the Navy. These facilities provided rapid communication between the Navy Department and the commanders of squadrons, when in port. This permitted the Navy Department to keep its commanders advised of the political situation, but lessened the amount of discretion allowed them." (Howeth, *History of Communications-Electronics*, pp. 10-11).

[17] For example, Admiral Nelson established a rudimentary network of ships to keep an eye on the French/Spanish fleet in Cádiz in the lead-up to the Battle of Trafalgar as his ships remained out of sight from the enemy.
[18] Norman Friedman, "Netting and Navies: Achieving a Balance," paper presented at the Royal Australian Navy Sea Power Conference, Sydney, Australia, February 2006, p. 6.
[19] Norman Friedman, "Netting and Navies."
[20] Loren Thompson, *Networking the Navy: A Model for Modern Warfare* (Arlington, VA: Lexington Institute, 2003).
[21] Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War* (Washington, D.C.: Department of Defense Command and Control Research Program, 2002), pp. 509-512.
[22] N.A.M. Rodger, presentation at the Royal Australian Navy King-Hall Naval History Conference, Sydney /Canberra, Australia, 24 and 26-27 July 2007, p. 6.
[23] It is difficult to overstate the importance of the invention of the telegraph. For the first time ever, it was possible to move information faster than people or goods. Therefore it is not difficult to understand how proponents – as well as users – of the telegraph did not thoughtfully consider the unintended consequences of its use.
[24] Rodger, presentation to King-Hall Conference, Canberra, January 24, 2007 (from Galdorisi notes transcription).
[25] Rodger, presentation to King-Hall.
[26] Former CNO, Admiral Vern Clark described FORCEnet as an "operational construct and architectural framework for naval warfare in the information age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force." Admiral Vern Clark, "Sea Power 21: Projecting Decisive Joint Capabilities," *United States Naval Institute Proceedings*, October 2002.
[27] *Military Transformation: A Strategic Approach* (Washington, D.C.: Department of Defense, 2003), pp. 1-36, accessed at: http://www.oft.osd.mil. This publication is the capstone publication of the Office of Force Transformation, U.S. Department of Defense. For further information on interoperability and the levels of interoperability see Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, pp. 107-121.
[28] Galdorisi and Sutton, "Achieving the Global Maritime Partnership," p.69.
[29] Deputy Chief of Naval Operations (Communication Networks), "FORCEnet for the 1000-Ship Navy," *Memorandum for Director, Warfare Integration Division (N6F)* (Washington D.C.: Department of the Navy, Office of the Chief of the Naval Operations, 24 July 2006).
[30] Dave Alberts, statement made at the annual 7th International Command and Control Research and Technology Symposium, Québec City, Canada, September 2002.
[31] Alberts, et. al., *Understanding Information Age Warfare*, p. 277.
[32] Alberts, et. al., *Understanding Information Age Warfare*, 278-279.
[33] Non-traditional allies refers to military and non-military organizations that the U.S. military and the U.S. Navy do not have a historical partnership with. Traditional allies would be NATO nations with whom the U.S. has worked closely to shape operational and technical requirements.
[34] Paul Mitchell, "Small Navies and Network-Centric Warfare: Is There a Role?" *Naval War College Review*, spring 2003, pp. 83-99. See also Gordon Adams et al., *Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability* (Washington, D.C.: National Defense University, 2004); and, in particular, Rob de'Wijk, "European Military Reform for a Global Partnership," *The Washington Quarterly*, 27: 1, 2003, pp. 197-210, for specific challenges faced by European navies in effectively partnering with the U.S. Navy.
[35] Brad Carter and Deb Harlor, "Combined Operations Wide Area Network (COWAN)/ Combined Enterprise Regional Information Exchange System (CENTRIXS)," *Biennial Review* (San Diego, CA: Space and Naval Warfare Systems Center San Diego, 2003), p. 87.
[36] Gordon Van Hook, "How to Kill a Good Idea," *United States Naval Institute Proceedings*, October 2007, p. 34. Captain Van Hook notes the limitations of CENTRIXS, stating: "We must move beyond limited approaches to link a few secure common systems with software applications like CENTRIXS, and get to a fully integrated regional picture from ports to harbors and into the commons."
[37] For more on FORCEnet see the following: *FORCEnet: A Functional Concept for Command and Control in the 21st Century* (Norfolk, VA: Naval Network Warfare Command, 2006) available at

http://www.enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R and FORCEnet*: A Functional Concept for Command and Control in the 21st Century: Annex Version 20 June 2006* (Norfolk, VA: Naval Network Warfare Command, 2006).

[38] Van Hook, "How to Kill a Good Idea," p. 33. Captain Van Hook, drawing on his experience as a destroyer squadron commander where he worked with coalition partners, emphasized the importance of a cooperative approach to instantiating the global maritime partnership, noting that the U.S. should; "Encourage regional maritime security arrangements to form at the grassroots level, without overt U.S. leadership."

[39] See The Technical Cooperation Program: TTCP document DOC-SEC-3-2005, *A Beginner's Guide to the Technical Cooperation Program*, September 1, 2005, accessed at: http://www.dtic.mil/ttcp/. The statistics alone give some indication of the scope of this effort; five nations involved, 11 technology and systems groups formed, 80 technical panels and action groups up and running, 170 organizations involved, and 1200 scientists and engineers directly accessed.

[40] Admiral James Stavridis, "Deconstructing War," *U.S. Naval Institute Proceedings*, December 2005.

SPAWAR
Systems Center
San Diego

13th ICCRTS: C2 for Complex Endeavors

Networking the Global Maritime Partnership

Mr. George Galdorisi, Dr. Stephanie Hszieh, Mr. Terry McKearney
Space and Naval Warfare Systems Center, San Diego
June 19, 2008

SSC San Diego … on Point and at the Center of C4ISR

Perspective

- The globalization of commerce has made the need for a global maritime partnership (GMP) an *urgent* requirement to support worldwide prosperity.
- Networking navies is a *necessary condition* for a GMP but technological advances among navies have often been uneven – impeding effective networking.
- We have “beta-tested,” and will share, one methodology for networking navies more effectively.
- While we will present results from a naval perspective, the C4ISR lessons-learned from this effort can readily be extrapolated to other complex endeavors.

…but first, is coalition networking really that important to the United States Navy?....

"We cannot talk about maritime power without talking about the cooperation between the U.S. Navy and our coalition partners."

Admiral Gary Roughead
Chief of Naval Operations
NLUS Sea-Air-Space Symposium
Washington, D.C.
March 18, 2008

“Building partner capability is important to our Navy. We must endeavor to improve our networking capability with partners, especially our ability to exchange data at high rates.”

Admiral John Greenert
Commander, Fleet Forces Command
NLUS Sea-Air-Space Symposium
Washington, D.C.
March 18, 2008

"What we build and what we subsequently sell to foreign navies used to be low priority for the Naval Sea Systems Command. Today, with the Thousand Ship Navy and the Global Maritime Partnership, this is now a huge part of what we do."

Vice Admiral Paul Sullivan
Commander, Naval Sea Systems Command
NLUS Sea-Air-Space Symposium
Washington, D.C.
March 20, 2008

“The Navy International Program Office (Navy IPO) is an increasingly important part of the ASN RD&A portfolio. Maritime forces foster relationships that help sustain confidence in the global system and allow it to flourish.”

Mr. John Thackrah
Acting ASN RD&A
NLUS Sea-Air-Space Symposium
Washington, D.C.
March 20, 2008

No Navy Stands Alone and Networking Navies Effectively is a Necessary Condition for a Global Maritime Partnership

07

“The power to create a voluntary network of maritime forces is within our grasp, We have the capability to seize on our inherent nature of cooperation at sea and, together, overcome transnational actors who threaten the very fabric of global safety and security.”

Admiral Michael Mullen
U.S. Navy Chief of Naval Operations
RUSI Future Maritime Warfare Conference
December 13, 2005

Networking the Global Maritime Partnership

- Globalization has brought nations closer together and increased world-wide prosperity
- Navies under-gird the ability of nations to trade across the global commons
- Globalization has facilitated all forms of international terrorism
- No one navy can police the global commons – a Global Maritime Partnership is needed

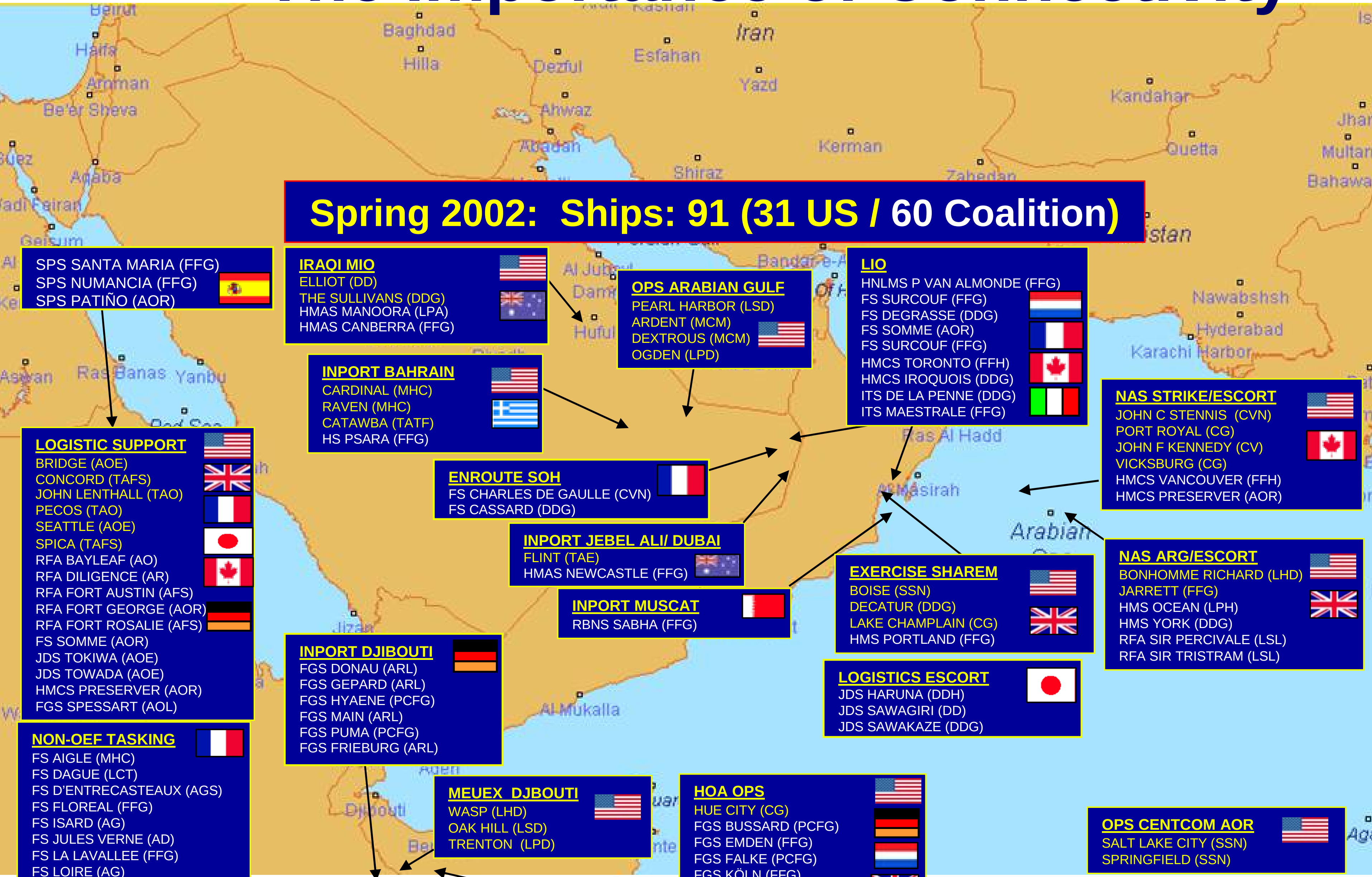
Networking the Global Maritime Partnership

- Navies working together to defeat terrorists must be effectively networked
- This networking is crucial to develop a common operational picture and to self-synchronize
- Emerging C4ISR technologies are critical to networking navies
- The fact that navies have led networking at sea often obscures technological challenges

“The significant involvement of coalition forces in Operation Enduring Freedom – including over 100 ships deployed in Central Asia for an extended period – has reemphasized the requirement for improved internet protocol data systems interoperability with allied and coalition forces.”

Admiral Robert Natter
Commander, Fleet Forces Command
SSC Charleston *Combat Clips*
Summer 2002

The Importance of Connectivity



Spring 2002: Ships: 91 (31 US / 60 Coalition)

🇪🇸
SPS SANTA MARIA (FFG)
SPS NUMANCIA (FFG)
SPS PATIÑO (AOR)

IRAQI MIO 🇺🇸 🇦🇺
ELLIOT (DD)
THE SULLIVANS (DDG)
HMAS MANOORA (LPA)
HMAS CANBERRA (FFG)

OPS ARABIAN GULF 🇺🇸
PEARL HARBOR (LSD)
ARDENT (MCM)
DEXTROUS (MCM)
OGDEN (LPD)

LIO 🇳🇱 🇫🇷 🇨🇦 🇮🇹
HNLMS P VAN ALMONDE (FFG)
FS SURCOUF (FFG)
FS DEGRASSE (DDG)
FS SOMME (AOR)
FS SURCOUF (FFG)
HMCS TORONTO (FFH)
HMCS IROQUOIS (DDG)
ITS DE LA PENNE (DDG)
ITS MAESTRALE (FFG)

INPORT BAHRAIN 🇺🇸 🇬🇷
CARDINAL (MHC)
RAVEN (MHC)
CATAWBA (TATF)
HS PSARA (FFG)

NAS STRIKE/ESCORT 🇺🇸 🇨🇦
JOHN C STENNIS (CVN)
PORT ROYAL (CG)
JOHN F KENNEDY (CV)
VICKSBURG (CG)
HMCS VANCOUVER (FFH)
HMCS PRESERVER (AOR)

LOGISTIC SUPPORT 🇺🇸 🇬🇧 🇫🇷 🇯🇵 🇨🇦 🇩🇪
BRIDGE (AOE)
CONCORD (TAFS)
JOHN LENTHALL (TAO)
PECOS (TAO)
SEATTLE (AOE)
SPICA (TAFS)
RFA BAYLEAF (AO)
RFA DILIGENCE (AR)
RFA FORT AUSTIN (AFS)
RFA FORT GEORGE (AOR)
RFA FORT ROSALIE (AFS)
FS SOMME (AOR)
JDS TOKIWA (AOE)
JDS TOWADA (AOE)
HMCS PRESERVER (AOR)
FGS SPESSART (AOL)

ENROUTE SOH 🇫🇷
FS CHARLES DE GAULLE (CVN)
FS CASSARD (DDG)

INPORT JEBEL ALI/ DUBAI 🇦🇺
FLINT (TAE)
HMAS NEWCASTLE (FFG)

INPORT MUSCAT 🇧🇭
RBNS SABHA (FFG)

EXERCISE SHAREM 🇺🇸 🇬🇧
BOISE (SSN)
DECATUR (DDG)
LAKE CHAMPLAIN (CG)
HMS PORTLAND (FFG)

NAS ARG/ESCORT 🇺🇸 🇬🇧
BONHOMME RICHARD (LHD)
JARRETT (FFG)
HMS OCEAN (LPH)
HMS YORK (DDG)
RFA SIR PERCIVALE (LSL)
RFA SIR TRISTRAM (LSL)

INPORT DJIBOUTI 🇩🇪
FGS DONAU (ARL)
FGS GEPARD (ARL)
FGS HYAENE (PCFG)
FGS MAIN (ARL)
FGS PUMA (PCFG)
FGS FRIEBURG (ARL)

LOGISTICS ESCORT 🇯🇵
JDS HARUNA (DDH)
JDS SAWAGIRI (DD)
JDS SAWAKAZE (DDG)

NON-OEF TASKING 🇫🇷 🇬🇧
FS AIGLE (MHC)
FS DAGUE (LCT)
FS D'ENTRECASTEAUX (AGS)
FS FLOREAL (FFG)
FS ISARD (AG)
FS JULES VERNE (AD)
FS LA LAVALLEE (FFG)
FS LOIRE (AG)
FS SIROCO (LSD)
FS VAR (AOR)
FS VERSEAU (MHC)
HMS SPLENDID (SSN)

MEUEX DJBOUTI 🇺🇸
WASP (LHD)
OAK HILL (LSD)
TRENTON (LPD)

HOA OPS 🇺🇸 🇩🇪 🇳🇱 🇬🇧 🇫🇷
HUE CITY (CG)
FGS BUSSARD (PCFG)
FGS EMDEN (FFG)
FGS FALKE (PCFG)
FGS KÖLN (FFG)
HNLMS VAN AMSTEL (FFG)
HMS CAMPBELTOWN (FFG)
FS SAPHIR (SSN)

OPS CENTCOM AOR 🇺🇸
SALT LAKE CITY (SSN)
SPRINGFIELD (SSN)

ENROUTE OUTCHOP 🇬🇧
HMS SCOTT (AGS)

INPORT SEYCHELLES 🇩🇪
FGS BAYERN (FFG)

Technological Advances Among Navies Have Been Uneven – Impeding Effective Networking Between Navies

"Is there a place for small navies in network-centric warfare? Will they be able to make any sort of contribution in multinational naval operations of the future? Or will they be relegated to the sidelines, undertaking the most menial of tasks, encouraged to stay out of the way– or stay at home?…The "need for speed" in network-centric operations places the whole notion of multinational operations at risk."

Professor Paul Mitchell
Former Director of Academics
Canadian Forces College
Naval War College Review – Spring 2003

"There's no one in the Navy leadership who thinks that the Navy can do this alone…if we want to embrace the thousand-ship navy [concept] and maritime security initiatives, we have to make sure that we don't leave a large majority of our partners behind."

Vice Admiral Mark Edwards
Deputy Chief of Naval Operations for
Communication Networks (N6)
Seapower Magazine
April 2008

Technological Advances and Networking

- Coalition partners working with the U.S. Navy often want to know the “price of *admission*”
- From the U.S. perspective it is more about the “price of *omission*” if we can not work together
- It is not ship hulls or aircraft airframes that enable this – but C4ISR technologies
- If each coalition partner develops these technologies independently, chaos can ensue

Technological Advances and Networking

- The “need for speed” often drives each navy to push technology forward independently
- Coordinated technological development in parallel offers one promising solution to this
- This must then translate to parallel acquisition of systems that are mutually compatible
- This sounds great in theory, but is there a “best-practice” model that we can examine?

We Have “Beta-Tested” and will Share *one* Methodology for Networking Navies More Effectively

NAVY
AUSTRALIA

The Challenge

"Expanded cooperation with the maritime forces of other nations requires more interoperability with multinational partners possessing varying levels of technology. The *Global Maritime Partnership* initiative will serve as a catalyst for increased international interoperability in support of cooperative maritime security."

Admiral Gary Roughead
Chief of Naval Operations
A Cooperative Strategy for 21st Century Seapower
October 2007

Our "Beta-Test" Under the Auspices of The Technical Cooperation Program: One Path to "Building the Networks"

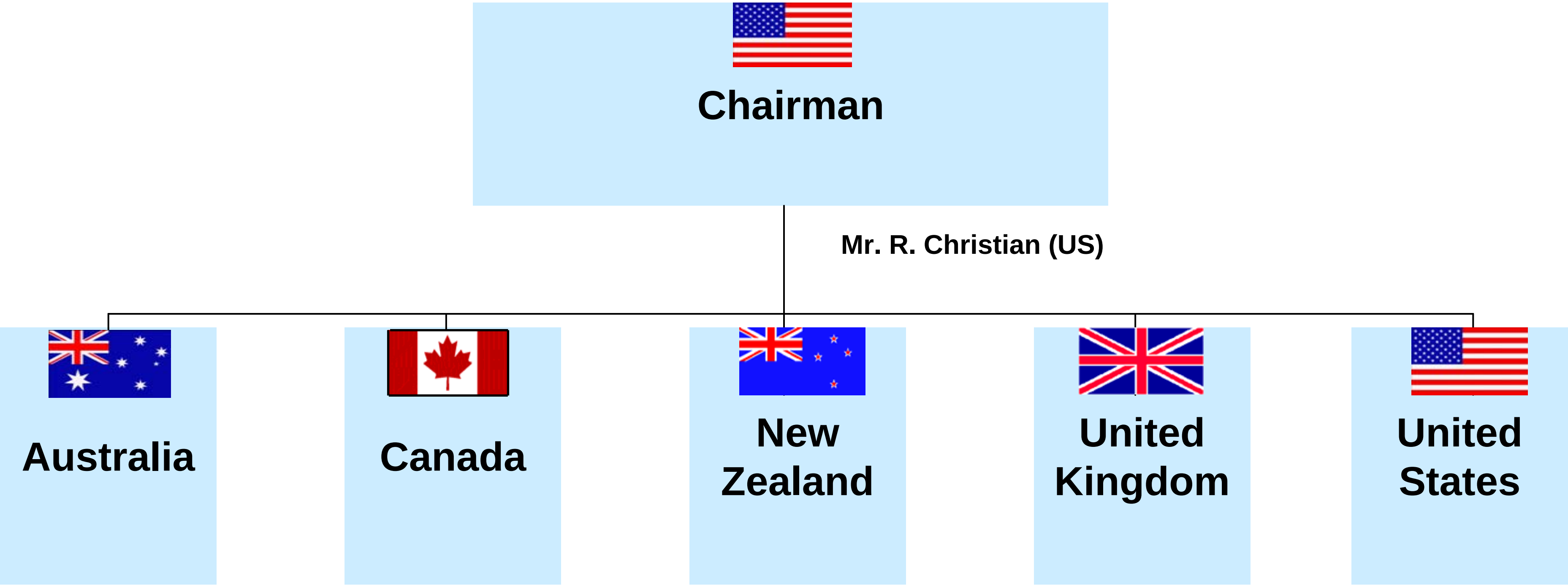
One Model for International Defense Cooperation: MAR AG-1/AG-6

MAR Action Group 1: “Maritime Network Centric Warfare”

MAR Action Group 1

- Maritime Network Centric Warfare
  - Open ended
- Focus on “bounding the problem”
  - Good product
- Proof of concept through multilateral analysis
- Warfighting scenarios with traction for all
- Two Studies
  - Broad Issues: First Principles of NCW
  - Tactical Level Analysis: MIO/ASW/ASuW

AG-1 Membership



Chairman

Mr. R. Christian (US)

Australia

Canada

New Zealand

United Kingdom

United States

Australia:

Dr. C. Davis (NL)
Ms. S. Andrijich (M)
Ms. M. Hue (M)
Dr. I. Grivell (M)
Dr. D. Sutton (M)
Dr. M. Fewell (M)

Canada:

Mr. P. Sutherland (NL)
Mr. R. Burton (M)
Mr. M. Hazen (M)
Mr. B. Richards (M)

New Zealand:

Dr. D. Galligan (NL)
Mr. C. Phelps (M)

United Kingdom:

Mr. A. Sutherland (NL)
Mr. P. Marland (M)
Mr. R. Lord (M)

United States:

Mr. J. Shannon (NL)
Dr. R. Klingbeil (M)
Dr. S. Dickinson (M)
Mr. G. Galdorisi (M)*

Notes: NL = National Leader
M = Member

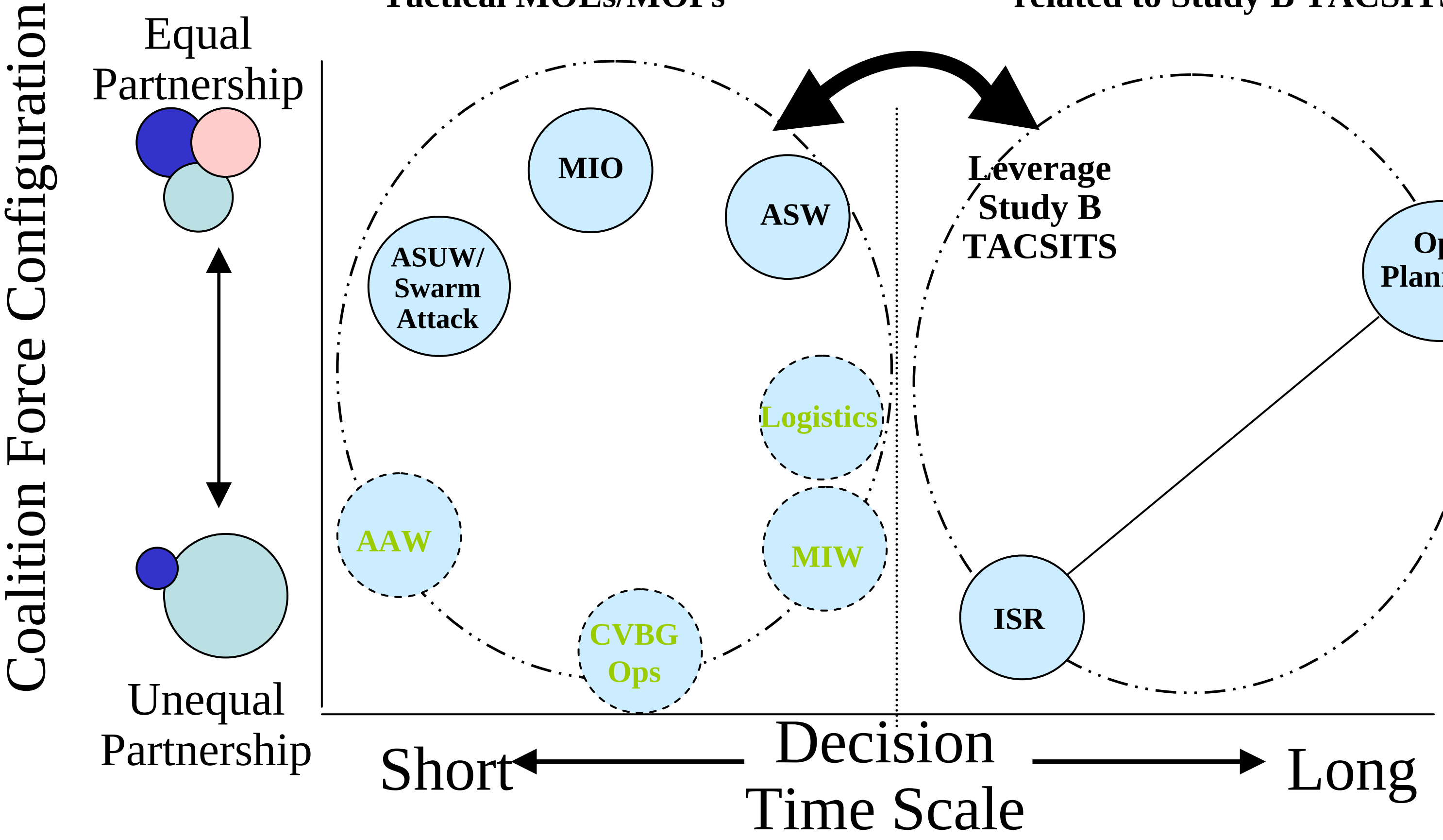
Two Component Studies

Study B (Tactical Level)

- TACSIT-based analysis (relevant, littoral)
- Sense-Decide-Respond
- Connectivity dependence
- Tactical MOEs/MOPs

Study A (Broad Issues)

- First Principles in NCW
- Quantitative analysis of alternative networking options in ISR/Operational Planning, as related to Study B TACSITS



MAR AG-1 Study B
Tactical Level Analysis

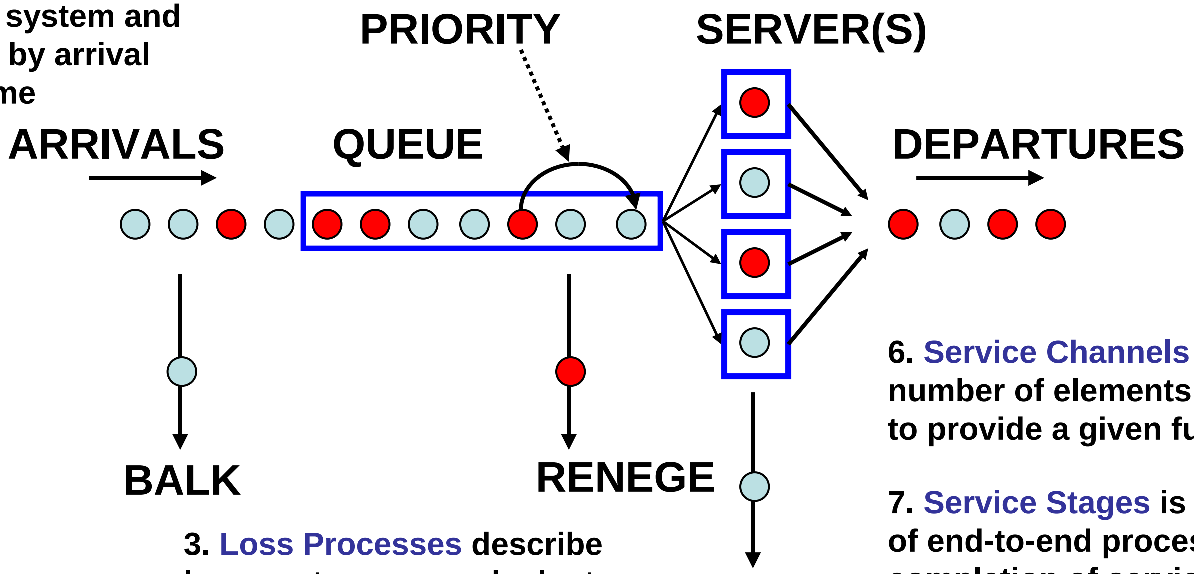
Queuing System for MIO

4. Queue Discipline describes how a customer is selected for service once in queue (FIFO, priorities, etc.)

5. System Capacity is the maximum size of a queue; finite or infinite

2. Service Pattern is described by service rate or service time

1. Arrival Pattern describes the input to the queuing system and is typically specified by arrival rate or interarrival time



🔴 TOI

⚪ Non-TOI

6. Service Channels are the number of elements available to provide a given function

7. Service Stages is the set of end-to-end processes for completion of service

3. Loss Processes describe how customers can be lost (balking and reneging)

KEY QUEUEING METRICS:

- Probability of a customer acquiring service
- Waiting time in queue until service begins
- Loss rate due to either balking or reneging

Queueing Theory interrelates key system characteristics and can be used to identify where investment should be made to improve performance and effectiveness

ASW TACSIT Analysis

Improving ASW Effectiveness – NCASW Concepts and Hypotheses

1 Shared Situational Awareness (SSA)

Network- enabled Shared Situational Awareness (SSA) can reduce false contact loading thereby increasing ASW effectiveness.

2 Collaborative Information Environment (CIE)

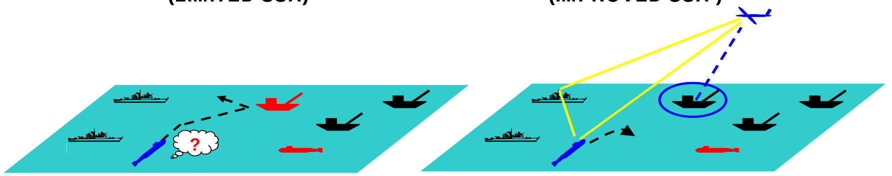
Sensor operators in a network-enabled collaborative environment can reach-back to ASW experts to improve target and non-target classification performance.

Queueing Theory can provide an intuitive mathematical and physical framework for the analysis of any military system or operation that can be characterized as a "waiting line" or a "demand-for-service."

False Target Reduction Concept

PLATFORM-CENTRIC ASW
(LIMITED SSA)

NETWORK-CENTRIC ASW
(IMPROVED SSA)



Submarine's search track plan is interrupted due to false contact investigation

Submarine avoids unnecessary false contact investigation due to SSA

- Congestion of sonar, high workload
- Time to investigate false contacts
- Reduction of effective search rate
- Missed detections of targets

- Information is essential
- System to remove specified sensor contacts
- Can possibly lower detection threshold
- Increased probability of target detection

- Use sensor correlation across all appropriate platforms in a task group to reduce the number of non-target contacts presented to sensor operators.
- Reduce non-object false contacts, such as reverberation spikes and wrecks, by using acoustic models, in situ data, and local data bases.

Metric for SSA Concept Analysis

Reduce false contact loading on the ASW system by improving Shared Situational Awareness (SSA)

$P_{ASW} = P_{DET} * \underline{\underline{P_{CLASS}}} * P_{LOC} * P_{ATK}$

P_{CLASS} = $P_{ACQ\ CLASS}$ * P(T|t)

$P_{ACQ\ CLASS}$ = probability that the target acquires classification service

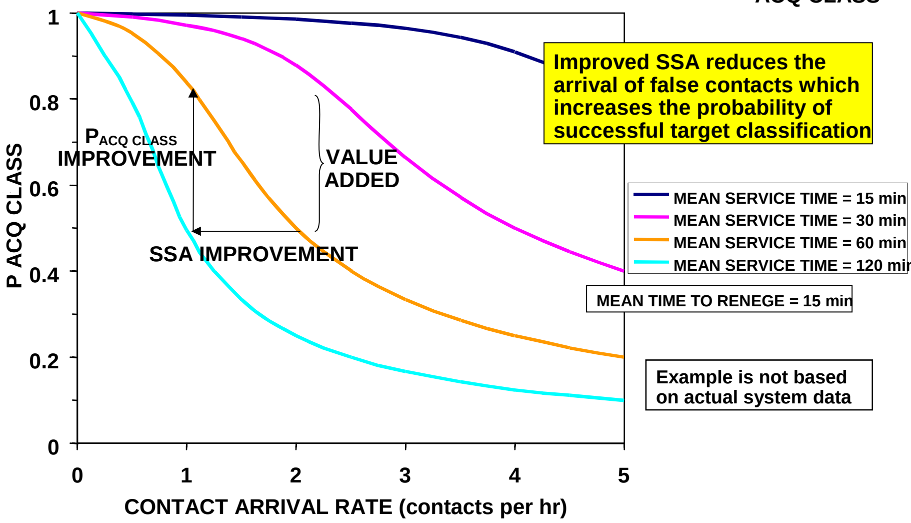
P(T|t) = probability of recognizing the target contact as the actual target of interest (experimental data required)

T = THREAT DECISION

t = true target

There are queueing aspects (waiting line/demand for service) in each of the terms in P_{ASW}

Effect Of Improved SSA and Service Time on $P_{ACQ\ CLASS}$



Improved SSA reduces the arrival of false contacts which increases the probability of successful target classification

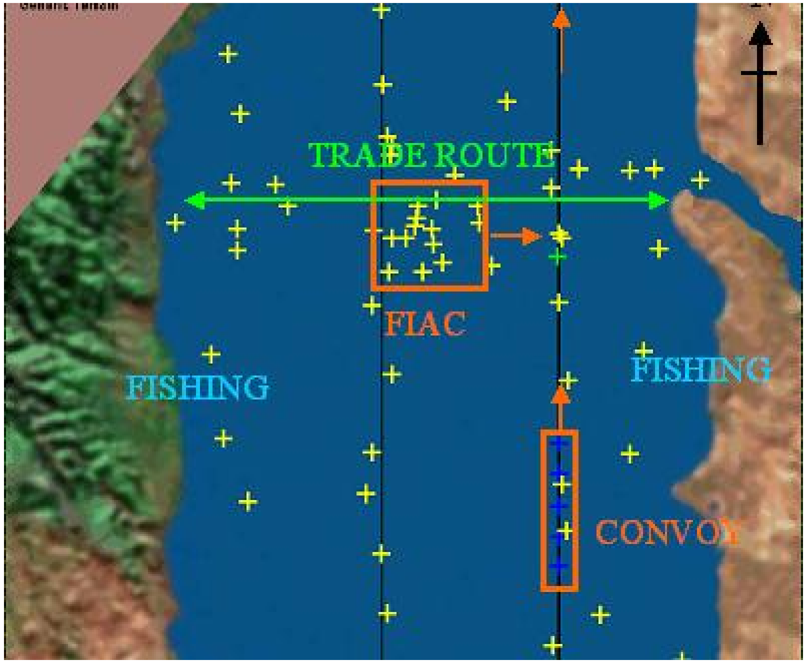
MEAN TIME TO RENEGE = 15 min

Example is not based on actual system data

ASuW/Swarm TACSIT Analysis

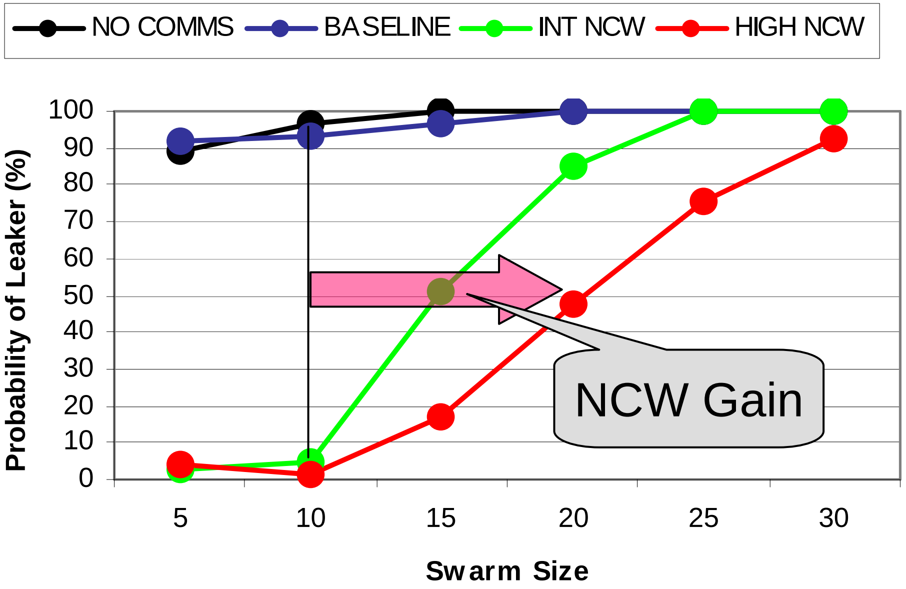
Tacsit: Blue force in restricted sea room is attacked by a swarm of FIAC. Network enabled Blue shared situational awareness and distributed targeting reduces the number of ‘leakers.’

Metrics: Probability of one or more FIAC reaching firing position against HVU. Fractions of FIAC leaking, and of Blue escorts damaged. Collateral damage.



Study has used MANA agent based model to represent the Swarm’s dynamic tactics, with four levels of Blue networking capability.

Sample Results: (30 knot FIAC)



- Intermediate and High levels of networking increase Force survivability versus Type 1 FIAC by factor of ≈9.
- Full results include dependencies on Red speed (leakers increase at 40 knots).

AG-1 Study “Takeaways”

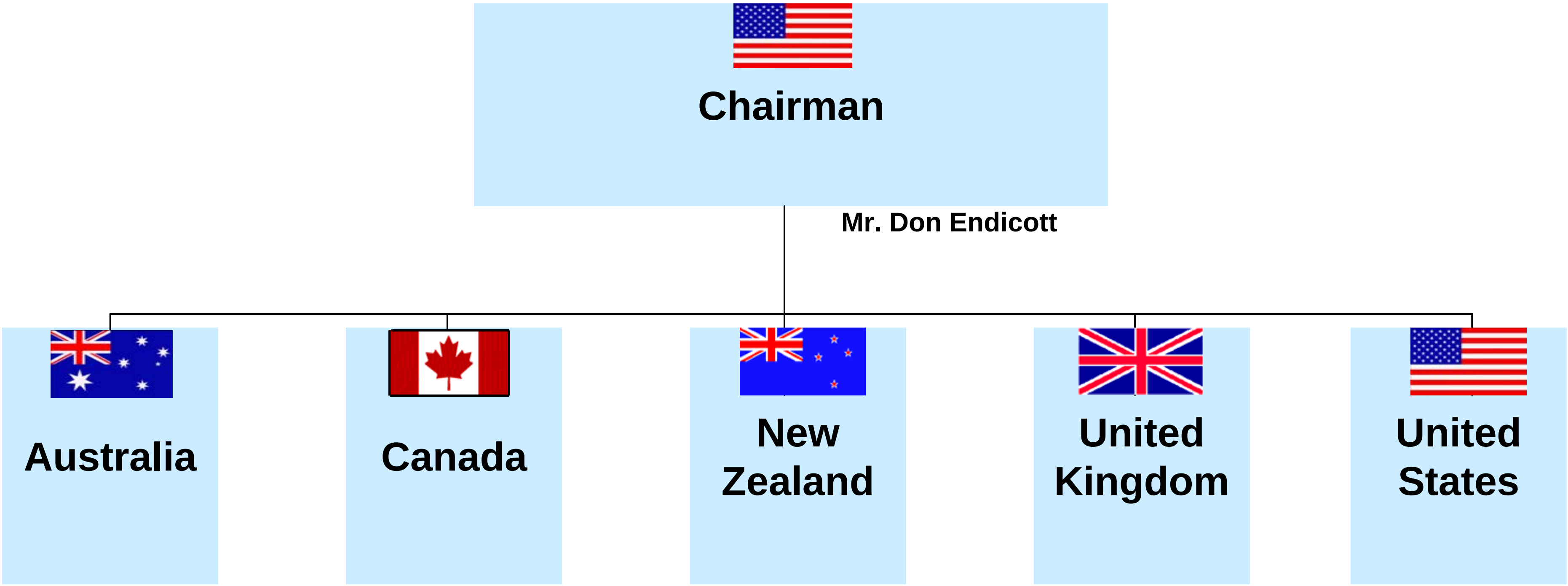
- Any analysis must begin with the recognition that there will likely be a significant networking capability gap between US and coalition partners
- This analysis must evaluate the impact of technology on a heterogeneously networked coalition naval force
- Networking would most benefit coalition naval forces in planning and re-planning, training, and reach-back to better intelligence

MAR Action Group 6 “FORCEnet Implications for Coalitions”

MAR AG-6 Direction and TOR

- Leverage AG-1work as much as possible
- Build on AG-1 work but add:
  - More specificity regarding ops and force structure
  - More granularity to analysis and modeling
- Work within a realistic operational scenario that all member nations would participate in
- Produce a product that informs national leadership and acquisition officials

AG-6 Membership



Chairman

Mr. Don Endicott

Australia

Canada

New Zealand

United Kingdom

United States

Dr. A. Knight (NL)
Ms. R. Kuster (M)
Ms. A. Quill (M)
Mr. M. Coombs (M)

Mr. R. Mitchell (NL)
Mr. M. Maxwell (M)
Dr. M. Lefrancois (M)

Dr. D. Galligan (NL)*
LCDR W. Andrew (M)

Mr. A. Sutherland (NL) *
Mr. P. Marland (M) *
Mr. M. Lanchbury (M)

Mr. D. Endicott (NL)
Mr. G. Galdorisi (M)*
Mr. P. Shigley (M)
Ms. M. Gmitruk (M)
Ms. K. Dufresne (M)
Mr. D. Zatt (M)
Dr. M. Green (M)
Mr. T. McKearney (M)
Ms. M. Schult (M)
Dr. S. Gallup (M)
Ms. M. Elliott (M)

Notes: NL = National Leader
M = Member
* = Former AG-1 member

What is FORCEnet?

FORCEnet is an "…operational construct and architectural framework for naval warfare in the information age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force."

Admiral Vern Clark
Former Chief of Naval Operations (2000-2005)
US Naval Institute Proceedings
October 2002

SPAWAR
Systems Center
San Diego

Premises

- FORCEnet will empower warfighters at all levels to execute more effective decision-making at an increased tempo, which will result in improved combat effectiveness and mission accomplishment.[1]
- The warfighting benefits of FORCEnet in a coalition context can be assessed through analysis and quantified to provide input to national balance of investment studies of the five member nations.[2]
- It is necessary that FORCEnet address current and near term information system requirements that support operations in the joint and coalition environments. **Coalition Communications was the clear number one priority** of all numbered fleet commanders and is a critical enabler in leveraging coalition partners in the GWOT.[3]

1. *FORCEnet: A Functional Concept for the 21st Century*
2. *MAR AG-6 Terms of Reference*
3. *FY 2006 Numbered Fleet Top C4 Requirements (CFFC/CPF consolidated message)*

Hypothesis

- Conducting modeling and simulation and detailed analysis to demonstrate the enhanced warfighting effectiveness of coalition partners (in this case – the AUSCANNZUKUS nations) netted in a FORCEnet environment can help inform national naval C4ISR acquisition programs.

Notional Coalition Order of Battle

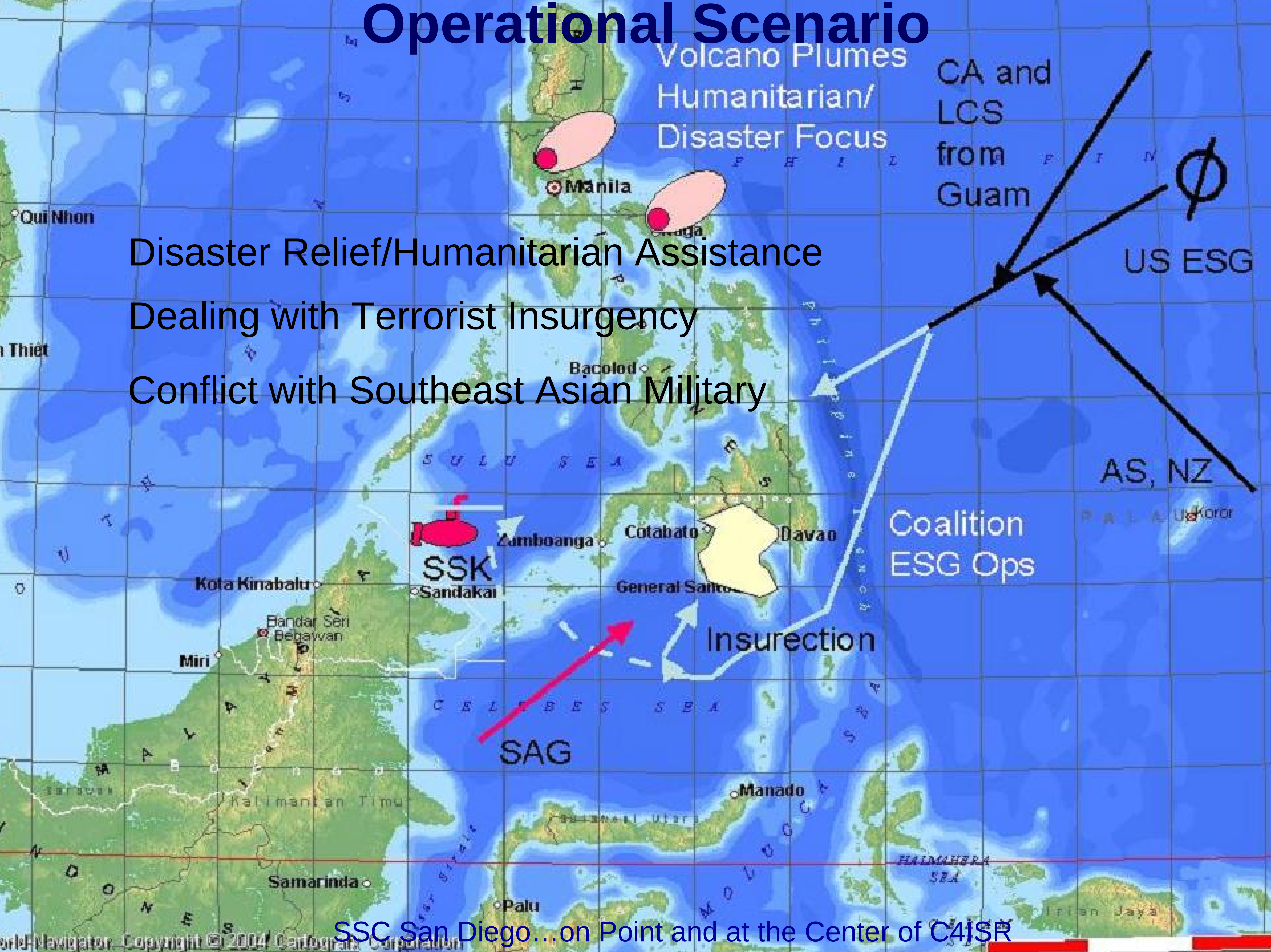
Australia	United Kingdom
•2 ANZAC Frigates •2 FFG •1 AWD	• 1 LPH/LPD • 2 LSD • 1 Replenishment Ship
Canada	**United States**
• 1 Destroyers • 2 Frigates • Replenishment Ship • Submarine	• 3 Amphibious Assault Ships • 1 Cruiser • 2 Destroyers • 3 Littoral Combat Ships • 1 Attack Submarine
New Zealand	
• 2 ANZAC Frigates • 1 Replenishment Ship • 1 Multi-role Vessel	

Operational Scenario

Disaster Relief/Humanitarian Assistance

Dealing with Terrorist Insurgency

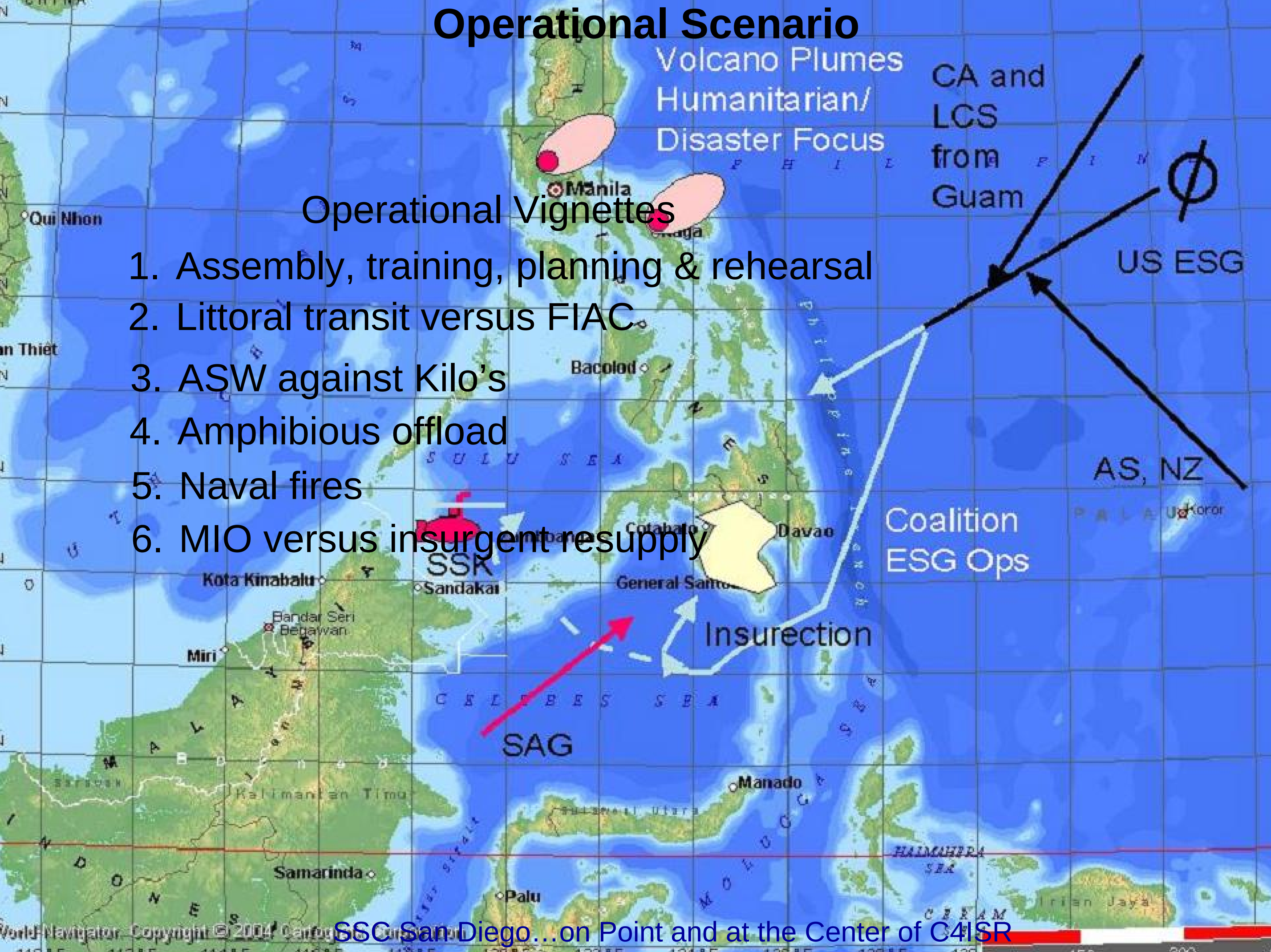
Conflict with Southeast Asian Military



Operational Scenario

Operational Vignettes

1. Assembly, training, planning & rehearsal
2. Littoral transit versus FIAC
3. ASW against Kilo’s
4. Amphibious offload
5. Naval fires
6. MIO versus insurgent resupply

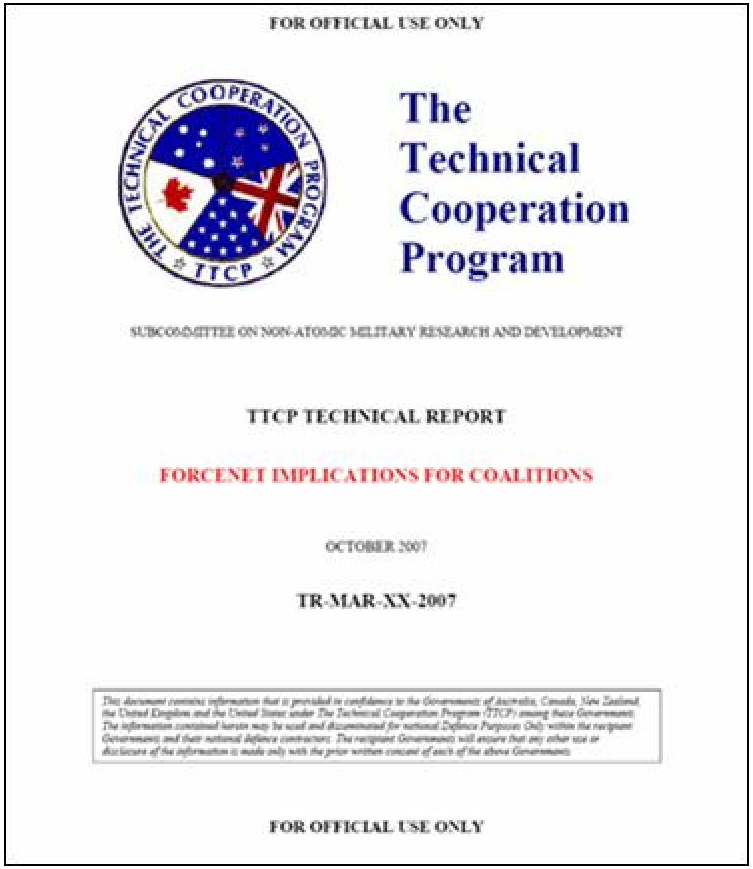


Initial Modeling Results - Summary

	Summary	Operational Impact	MoE Analysis
Assembly	Network capability limits time required to build force	Force can plan in advance of rendezvous, training time reduced	Total force at Fn Level1 reduced time required "in company" from 3 to 1 day
FIAC	Networking with increased ISR, flexible ROE enhances ability to counter	Gain in reducing probability of FIAC "leaker" attacking HVU	Fn level 0 or 1 little impact, Level 2 doubles size of swarm that can be countered
ASW	Increased networking impacts in both planning and common operational picture	Gains realizes in better networking of sensors and ISR assets (MPA, helo)	Fn Level 1 allowed OTH sensor monitoring and increase in predicted HVU survivability from .55 to .85.
Offload	Networking shared landing craft resources speeds delivery of on-cal relief supplies	Flexibility in delivering supplies to beach as HA mission unfolds	Fn Level 3 produced impact as all landing craft assets were able to service any supplying ship
Fires	Call-For- Fire process evolves from voice to digital data exchange	Reduced time allows for improved initial accuracy, less chance of targets escaping	Time to engage reduced from 55 min (Fn Level 0) to 2 min (Fn Level 3)
MIO	Range of networked capabilities for detection, tracking, and search of CCOIs have potential for improved performance	Better CCOI tracking through enhanced planning, asset management. Boarding party tools for personal safety and reachback into HQ databases	Probability of acquiring CCOI increased from .1 to .7 with Fn Level 1. Fn Level 2 needed for enhanced database tool and ISR integration

Capstone Report

- Ten chapters, eleven annexes
  - Including executive summary, bibliography
- Will describe study approach
  - Section on each vignette’s modeling
- Capabilities as described in Pastel Chart
  - Including issues relating to procurement of these capabilities
- Recommendations for further MAR efforts



FOR OFFICIAL USE ONLY

The Technical Cooperation Program

SUBCOMMITTEE ON NON-ATOMIC MILITARY RESEARCH AND DEVELOPMENT

TTCP TECHNICAL REPORT

FORCENET IMPLICATIONS FOR COALITIONS

OCTOBER 2007

TR-MAR-XX-2007

This document contains information that is provided in confidence to the Governments of Australia, Canada, New Zealand the United Kingdom and the United States under The Technical Cooperation Program (TTCP) among these Governments. The information contained herein may be used and disseminated for national Defence Purposes Only within the recipient Governments and their national defence contractors. The recipient Governments will ensure that any other use or disclosure of the information is made only with the prior written consent of each of the above Governments.

FOR OFFICIAL USE ONLY

Summary and Conclusions…
…and a suggested road ahead

"Why do we need a global network to provide maritime security? The short answer is the maritime domain is vital to most nations' economic prosperity and no nation can provide the requisite level of security by itself. It must be a shared endeavor among most of the world's nations if it is to be effective and efficient."

Admiral Michael Mullen
As U.S. Navy Chief of Naval Operations
RUSI Future Maritime Warfare Conference
December 13, 2005

Summary and Conclusions

1. Globalization has brought about the need for nations to work closely together
2. Today no navy stands alone & networking navies effectively is a necessary condition for a global maritime partnership
3. Technological advances among navies have been uneven – impeding effective networking between navies
4. We have “beta-tested” one methodology for networking navies more effectively and this model can be extrapolated to other nations and navies

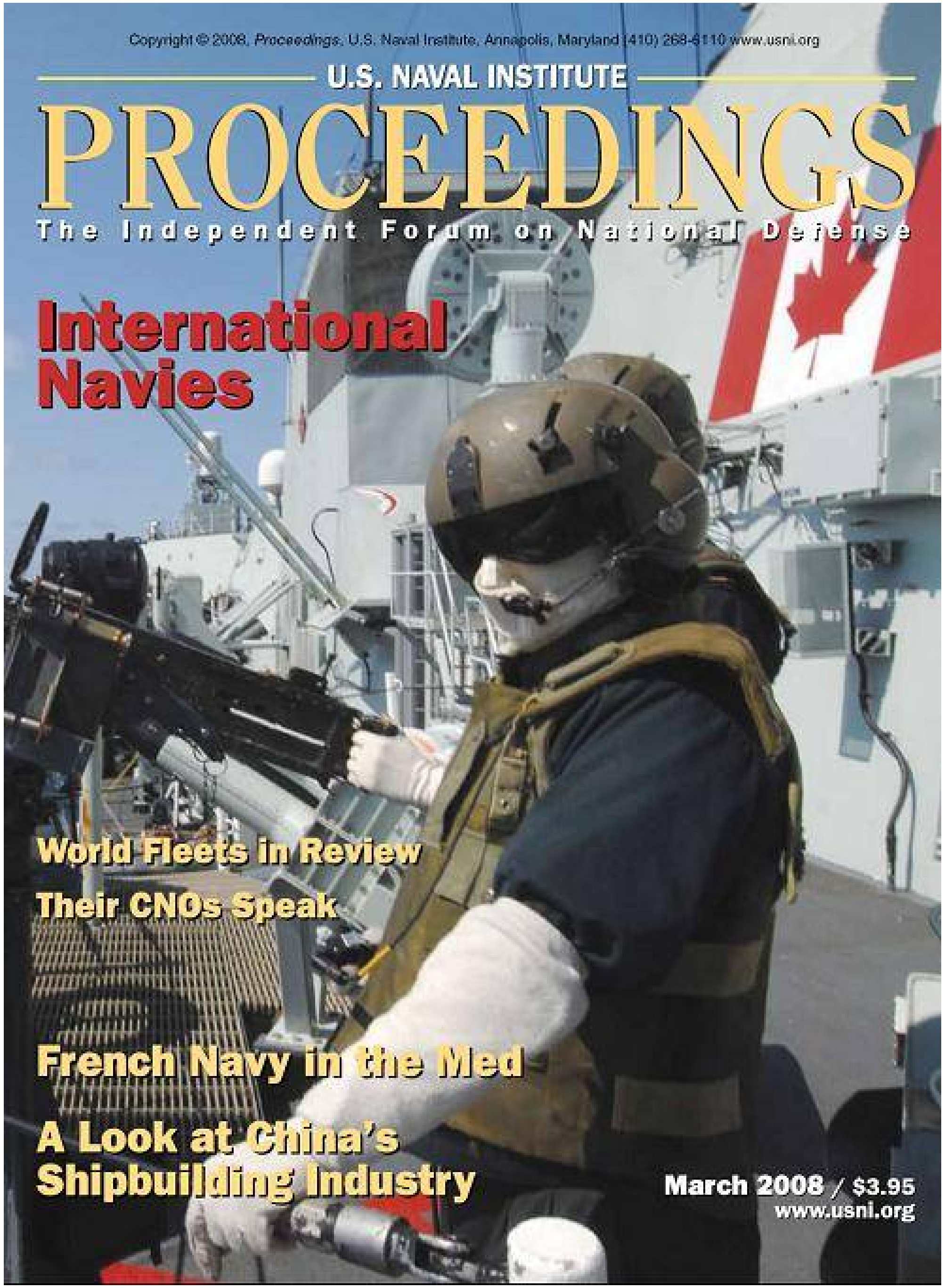
Summary and Conclusions

1. **Globalization has brought about the need for nations to work closely together**
2. **Today no navy stands alone & networking navies effectively is a necessary condition for a global maritime partnership**
3. **Technological advances among navies have been uneven – impeding effective networking between navies**
4. **We have "beta-tested" one methodology for networking navies more effectively and this model can be extrapolated to other nations and navies**

U.S. NAVAL INSTITUTE

PROCEEDINGS

The Independent Forum on National Defense



International Navies

World Fleets in Review

Their CNOs Speak

French Navy in the Med

A Look at China's Shipbuilding Industry

March 2008 / $3.95
www.usni.org

15
51
51

Backups

Our “Beta-Test” Under the Auspices of The Technical Cooperation Program: One Path to “Building the Networks”

The Technical Cooperation Program

- Defense-wide organization with emphasis on S&T
- Stable vehicle for collaborative efforts between and among five allies
- Valuable worldwide network of scientists and engineers that delivers technical advice
- Facilitates interoperability downstream through S&T collaboration

TTCP Current Groups

- Aerospace Systems (AER)
- Command, Control, Communications, & Information Systems (C3I)
- Chemical, Biological, and Radiological Defense (CBD)
- Electronic Warfare Systems (EWS)
- Human Resources and Performance (HUM)
- Joint Systems and Analysis (JSA)
- Land Systems (LAN)
- **Maritime Systems (MAR)**
- Materials and Processes Technology (MAT)
- Sensors (SEN)
- Conventional Weapons Technology (WPN)

MAR Construct

- **Technical Panels:**
  - TP-1: C2 and Information Management
  - TP-9: Sonar Technology
  - TP-10: Maritime ISR & Air Systems
  - TP-13: Mine Warfare and HF Acoustics
- **Action Groups:**
  - AG-1: Net Centric Warfare Study*
  - AG-2: Novel Maritime Platform Systems
  - AG-3: Torpedo Defense
  - AG-4: Surface Ship Air Defence Systems
  - AG-5: Force Protection
  - AG-6: FORCEnet Implications for Coalitions*

One Model for International Cooperation

- Maritime Action Groups
  - AG-1: “Maritime Network Centric Warfare”

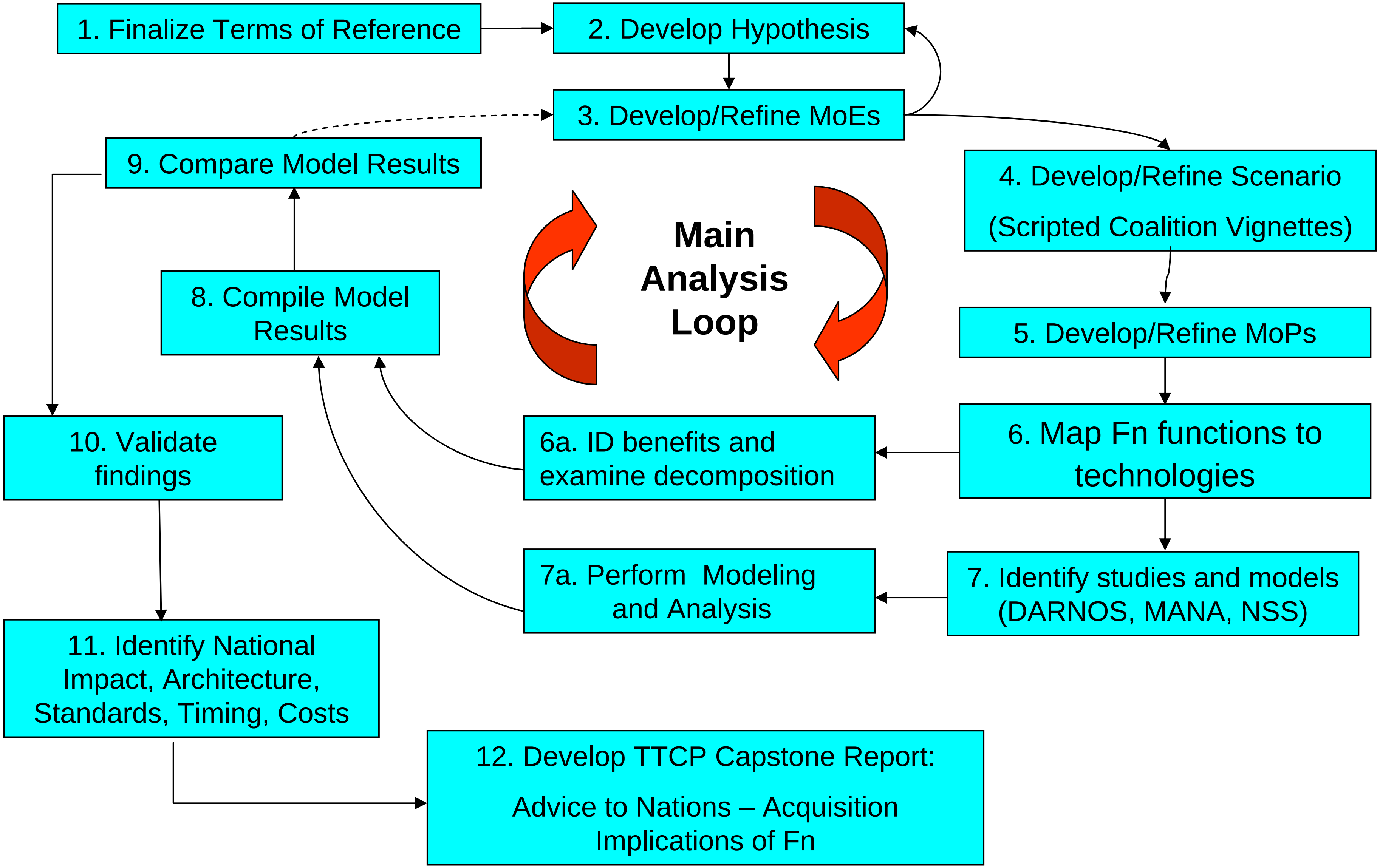
  …morphed into…

  - AG-6: “FORCEnet Implications for Coalitions”

"FORCEnet Implications for Coalitions"

- Group Composition
- Build on AG-1 Work
- Inform National Leadership
- Harmonize National Strategies

AG-6 Analysis Approach



1. Finalize Terms of Reference

2. Develop Hypothesis

3. Develop/Refine MoEs

4. Develop/Refine Scenario

(Scripted Coalition Vignettes)

5. Develop/Refine MoPs

6. Map Fn functions to technologies

6a. ID benefits and examine decomposition

7. Identify studies and models (DARNOS, MANA, NSS)

7a. Perform Modeling and Analysis

8. Compile Model Results

9. Compare Model Results

10. Validate findings

11. Identify National Impact, Architecture, Standards, Timing, Costs

12. Develop TTCP Capstone Report:

Advice to Nations – Acquisition Implications of Fn

Main Analysis Loop

Capability Stepping Stones to FORCEnet

Based on Fn Concept Document

Notional USN timeline as of 23 January 2007

Full IT21

"Online"

- IP Reach Back
- Local Area Networks
- Wideband Receive
- RF Management
- Survivable comms

Level 0

Today

Net Connected

"Improved decision making"

- Web-based services
- Improved network reliability and performance
- Increased bandwidth
- Improved coalition operations and data sharing
- Tailorable situational awareness tools
- Standardized data exchange between domains
- Defense in depth

Level 1

FY07

Net Enabled

"Network based command and control"

- Multi-path and improved transport reliability
- Dynamic bandwidth mgmt
- Customized applications and data sources
- Common infrastructure and data exchange standards
- Improved data exchange across domains
- Enterprise management for asset analysis and repair
- Initial knowledge management and automated decision aids
- Assured sharing
- Distributed command and control operations
- Modular and open architecture

Level 2

FY10

Fully Net Ready

"Decision-making under undesirable conditions"

- Robust, reliable communication to all nodes
- Reliable, accurate and timely information on friendly, environmental, neutral and hostile units
- Storage and retrieval of authoritative data sources
- Robust knowledge management capability with direct access ability to raw data
- User-defined and shareable SA
- Distributed and collaborative command and control
- Automated decision aids to enhance decision making
- Information assurance
- Seamless cross-domain access and data exchange.
- Interoperability across all domains and agencies
- Autonomous and disconnected operations
- Automatic and adaptive diagnostic and repair
- Modular architecture to expedite new capabilities

Level 3

FY14

SPAWAR
Systems Center
San Diego

AG-6's FORCEnet Capabilities Roadmap

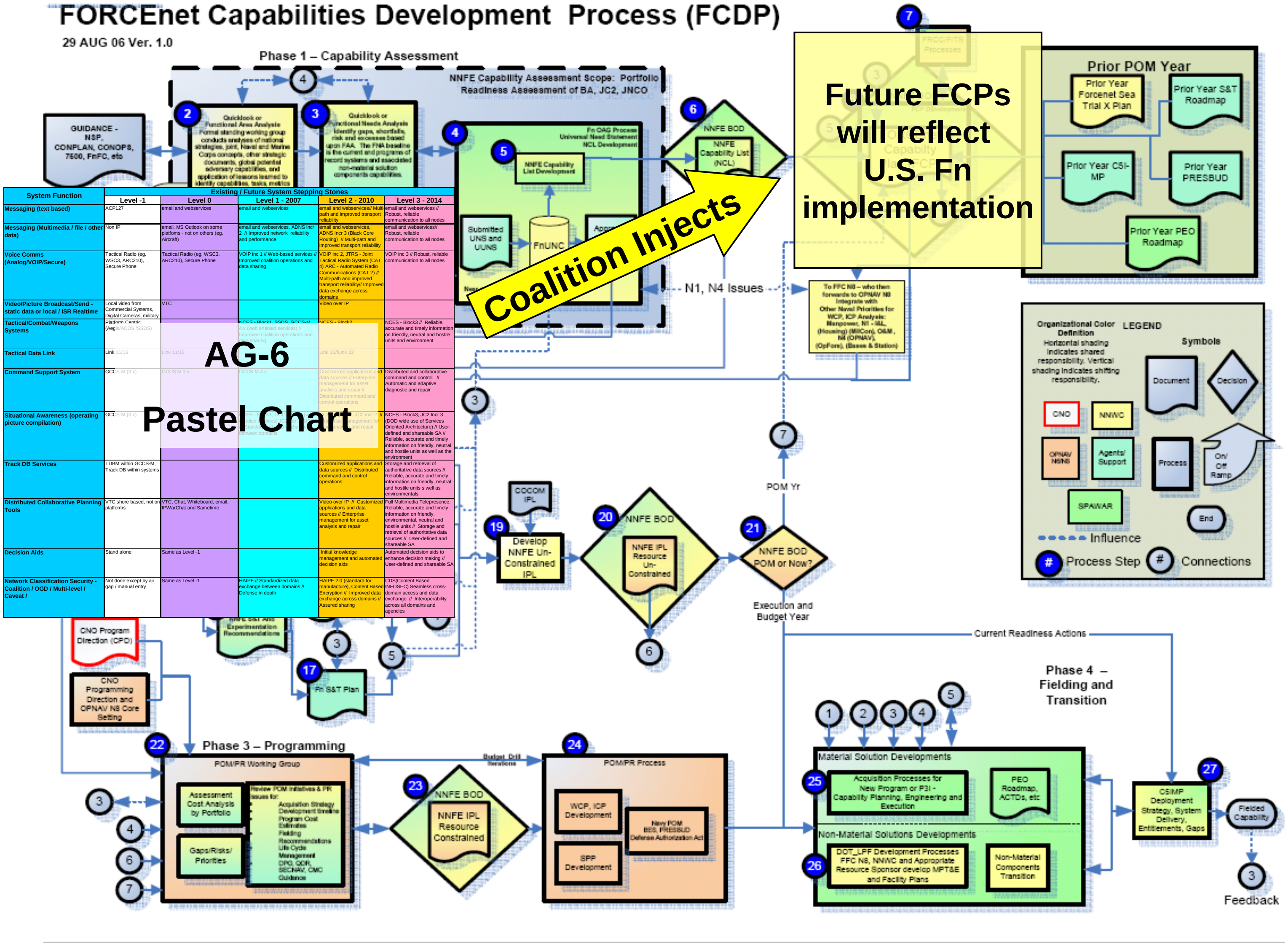
FORCEnet Levels

System Function	Existing / Future System Stepping Stones				
	Level -1	Level 0	Level 1 - 2007	Level 2 - 2010	Level 3 - 2014
Messaging (text based)	ACP127	email and webservices	email and webservices	email and webservices// Multi path and improved transport reliability	email and webservices // Robust, reliable communication to all nodes
Messaging (Multimedia / file / other data)	Non IP	email, MS Outlook on some platforms - not on others (eg. Aircraft)	email and webservices, ADNS incr 2 // Improved network reliability and performance	email and webservices, ADNS Incr 3 (Black Core Routing) // Multi-path and improved transport reliability	email and webservices// Robust, reliable communication to all nodes
Voice Comms (Analog/VOIP/Secure)	Tactical Radio (eg. WSC3, ARC210), Secure Phone	Tactical Radio (eg. WSC3, ARC210), Secure Phone	VOIP inc 1 // Web-based services // Improved coalition operations and data sharing	VOIP inc 2, JTRS - Joint Tactical Radio System (CAT 4) ARC - Automated Radio Communications (CAT 2) // Multi-path and improved transport reliability// Improved data exchange across domains	VOIP inc 3 // Robust, reliable communication to all nodes
Video/Picture Broadcast/Send - static data or local / ISR Realtime	Local video from Commercial Systems, Digital Cameras, military	VTC		Video over IP	
Tactical/Combat/Weapons Systems	Platform Centric (Aegis/ACDS /SSDS)		NCES - Block1, SSDS, GCCS-M 4.x (web enabled services) // Improved coalition operations and data sharing	NCES - Block2	NCES - Block3 // Reliable, accurate and timely information on friendly, neutral and hostile units and environment
Tactical Data Link	Link 11/16	Link 11/16		Link 16//Link 22	
Command Support System	GCCS-M (3.x)	GCCS M 3.x	GCCS M 4.x	Customized applications and data sources // Enterprise management for asset analysis and repair // Distributed command and control operations	Distributed and collaborative command and control // Automatic and adaptive diagnostic and repair
Situational Awareness (operating picture compilation)	GCCS-M (3.x)		NCES - Block1, GCCS-M 4.x (web enabled services),JC2 incr 1, UDOP // Standardized data exchange between domains	NCES - Block2, JC2 incr 2 // Enterprise management for asset analysis and repair	NCES - Block3, JC2 Incr 3 (DOD wide use of Services Oriented Architecture) // User-defined and shareable SA // Reliable, accurate and timely information on friendly, neutral and hostile units as well as the environment
Track DB Services	TDBM within GCCS-M, Track DB within systems			Customized applications and data sources // Distributed command and control operations	Storage and retrieval of authoritative data sources // Reliable, accurate and timely information on friendly, neutral and hostile units s well as environmentals
Distributed Collaborative Planning Tools	VTC shore based, not on platforms	VTC, Chat, Whiteboard, email, IPW arChat and Sametime		Video over IP // Customized applications and data sources // Enterprise management for asset analysis and repair	Full Multimedia Telepresence. Reliable, accurate and timely information on friendly, environmental, neutral and hostile units // Storage and retrieval of authoritative data sources // User-defined and shareable SA
Decision Aids	Stand alone	Same as Level -1		Initial knowledge management and automated decision aids	Automated decision aids to enhance decision making // User-defined and shareable SA
Network Classification Security - Coalition / OGD / Multi-level / Caveat /	Not done except by air gap / manual entry	Same as Level -1	HAIPE // Standardized data exchange between domains // Defense in depth	HAIPE 2.0 (standard for manufacture), Content Based Encryption // Improved data exchange across domains // Assured sharing	CDS(Content Based INFOSEC) Seamless cross-domain access and data exchange // Interoperability across all domains and agencies

23 Systems Functions

Existing/Future Systems Stepping Stones

FORCEnet Capabilities Development Process


FORCEnet Capabilities Development Process (FCDP)
29 AUG 06 Ver. 1.0
Phase 1 – Capability Assessment
GUIDANCE - NSP, CONPLAN, CONOPS, 7500, FnFC, etc
Quickook or Functional Area Analysis
Quicklook or Functional Needs Analysis Identify gaps, shortfalls, risk and excesses based upon FAA. The FNA baseline is the current and programs of record systems and associated non-material solution components capabilities.
NNFE Capability Assessment Scope: Portfolio Readiness Assessment of BA, JC2, JNCO
Fn OAG Process Universal Need Statement NCL Development
NNFE Capability List Development
Submitted UNS and UUNS
FnUNC
NNFE BOD
NNFE Capability List (NCL)
N1, N4 Issues
To FFC N8 – who then forwards to OPNAV N8 Integrate with Other Naval Priorities for WCP, ICP Analysis: Manpower, N1 - I&L (Housing) (MilCon), O&M, N4 (OPNAV), (OpFors), (Bases & Station)
Prior POM Year
Prior Year Forcenet Sea Trial X Plan
Prior Year S&T Roadmap
Prior Year CSI-MP
Prior Year PRESBUD
Prior Year PEO Roadmap
Organizational Color Definition
Horizontal shading indicates shared responsibility. Vertical shading indicates shifting responsibility.
LEGEND
Symbols
CNO
NNWC
OPNAV N6/N8
Agents/ Support
SPAWAR
Document
Decision
Process
On/ Off Ramp
End
Influence
Process Step
Connections
POM Yr
COCOM IPL
Develop NNFE Un-Constrained IPL
NNFE BOD
NNFE IPL Resource Un-Constrained
NNFE BOD POM or Now?
Execution and Budget Year
Current Readiness Actions
CNO Program Direction (CPD)
CNO Programming Direction and OPNAV N8 Core Setting
NNFE S&T And Experimentation Recommendations
Fn S&T Plan
Phase 3 – Programming
POM/PR Working Group
Assessment Cost Analysis by Portfolio
Gaps/Risks/ Priorities
Review POM Initiatives & PR Issues for:
Acquisition Strategy
Development timeline
Program Cost Estimates
Fielding Recommendations
Life Cycle Management
DPG, QDR, SECNAV, CMC Guidance
NNFE BOD
NNFE IPL Resource Constrained
Budget Drill Iterations
POM/PR Process
WCP, ICP Development
SPP Development
Navy POM BES, PRESBUD Defense Authorization Act
Phase 4 – Fielding and Transition
Material Solution Developments
Acquisition Processes for New Program or P3I - Capability Planning, Engineering and Execution
PEO Roadmap, ACTDs, etc
Non-Material Solutions Developments
DOT_LPF Development Processes FFC N8, NNWC and Appropriate Resource Sponsor develop MPT&E and Facility Plans
Non-Material Components Transition
CSIMP Deployment Strategy, System Delivery, Entitlements, Gaps
Fielded Capability
Feedback
1
2
3
4
5
6
7
17
19
20
21
22
23
24
25
26
27

Future FCPs will reflect U.S. Fn implementation

Coalition Injects

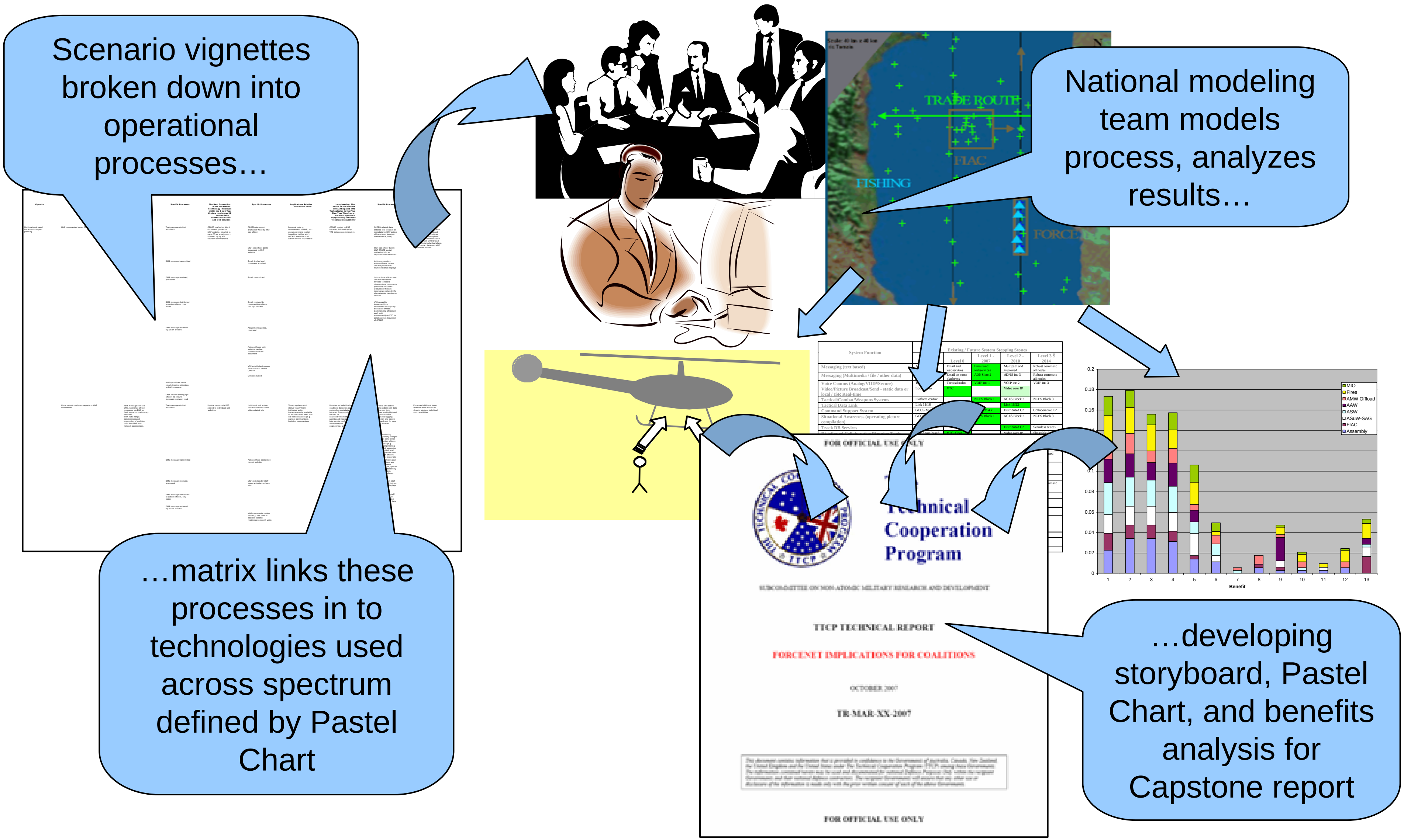
AG-6

Pastel Chart

System Function	Existing / Future System Stepping Stones				
	Level -1	Level 0	Level 1 - 2007	Level 2 - 2010	Level 3 - 2014
Messaging (text based)	ACP127	email and webservices	email and webservices	email and webservices// Multi-path and improved transport reliability	email and webservices // Robust, reliable communication to all nodes
Messaging (Multimedia / file / other data)	Non IP	email, MS Outlook on some platfoms - not on others (eg. Aircraft)	email and webservices, ADNS incr 2 // Improved network reliability and performance	email and webservices, ADNS Incr 3 (Black Core Routing) // Multi-path and improved transport reliability	email and webservices// Robust, reliable communication to all nodes
Voice Comms (Analog/VOIP/Secure)	Tactical Radio (eg. WSC3, ARC210), Secure Phone	Tactical Radio (eg. WSC3, ARC210), Secure Phone	VOIP inc 1 // Web-based services // Improved coalition operations and data sharing	VOIP inc 2, JTRS - Joint Tactical Radio System (CAT 4) ARC - Automated Radio Communications (CAT 2) // Multi-path and improved transport reliability// Improved data exchange across domains	VOIP inc 3 // Robust, reliable communication to all nodes
Video/Picture Broadcast/Send - static data or local / ISR Realtime	Local video from Commercial Systems, Digital Cameras, military	VTC		Video over IP	
Tactical/Combat/Weapons Systems	Platform Centric (Aegis/ACDS /SSDS)		NCES - Block1, SSDS, GCCS-M 4.x (web enabled services) // Improved coalition operations and data sharing	NCES - Block2	NCES - Block3 // Reliable, accurate and timely information on friendly, neutral and hostile units and environment
Tactical Data Link	Link 11/16	Link 11/16		Link 16//Link 22	
Command Support System	GCCS-M (3.x)	GCCS M 3.x	GCCS M 4.x	Customized applications and data sources // Enterprise management for asset analysis and repair // Distributed command and control operations	Distributed and collaborative command and control // Automatic and adaptive diagnostic and repair
Situational Awareness (operating picture compilation)	GCCS-M (3.x)		NCES - Block1, GCCS-M 4.x (web enabled services),JC2 incr 1, UDOP // Standardized data exchange between domains	NCES - Block2, JC2 incr 2 // Enterprise management for asset analysis and repair	NCES - Block3, JC2 Incr 3 (DOD wide use of Services Oriented Architecture) // User-defined and shareable SA // Reliable, accurate and timely information on friendly, neutral and hostile units as well as the environment
Track DB Services	TDBM within GCCS-M, Track DB within systems			Customized applications and data sources // Distributed command and control operations	Storage and retrieval of authoritative data sources // Reliable, accurate and timely information on friendly, neutral and hostile units s well as environmentals
Distributed Collaborative Planning Tools	VTC shore based, not on platforms	VTC, Chat, Whiteboard, email, IPWarChat and Sametime		Video over IP // Customized applications and data sources // Enterprise management for asset analysis and repair	Full Multimedia Telepresence. Reliable, accurate and timely information on friendly, environmental, neutral and hostile units // Storage and retrieval of authoritative data sources // User-defined and shareable SA
Decision Aids	Stand alone	Same as Level -1		Initial knowledge management and automated decision aids	Automated decision aids to enhance decision making // User-defined and shareable SA
Network Classification Security - Coalition / OGD / Multi-level / Caveat /	Not done except by air gap / manual entry	Same as Level -1	HAIPE // Standardized data exchange between domains // Defense in depth	HAIPE 2.0 (standard for manufacture), Content Based Encryption // Improved data exchange across domains // Assured sharing	CDS(Content Based INFOSEC) Seamless cross-domain access and data exchange // Interoperability across all domains and agencies

SPAWAR
Systems Center
San Diego

Vignette Modeling



Scenario vignettes broken down into operational processes…

National modeling team models process, analyzes results…

…matrix links these processes in to technologies used across spectrum defined by Pastel Chart

…developing storyboard, Pastel Chart, and benefits analysis for Capstone report

System Function	Existing / Future System Stepping Stones				
		Level 0	Level 1 - 2007	Level 2 - 2010	Level 3 Š 2014
Messaging (text based)	A[illegible]	Email and webservices	Email and webservices	Multipath and improved	Robust comms to all nodes
Messaging (Multimedia / file / other data)	[illegible]	Email on some platforms	ADNS inc 2	ADNS inc 3	Robust comms to all nodes
Voice Comms (Analog/VOIP/Secure)	T[illegible]	Tactical radio	VOIP inc 1	VOIP inc 2	VOIP inc 3
Video/Picture Broadcast/Send - static data or local / ISR Real-time	Loc[illegible]eo	VTC		Video over IP	
Tactical/Combat/Weapons Systems	Platform centric		NCES Block 1	NCES Block 2	NCES Block 3
Tactical Data Link	Link 11/16	[illegible]	[illegible]	Link 16/22	
Command Support System	GCCS-M[illegible]	[illegible]	[illegible]M 4.x	Distributed C2	Collaborative C2
Situational Awareness (operating picture compilation)	GCC[illegible]	[illegible]	[illegible]S Block 1	NCES Block 2	NCES Block 3
Track DB Services	[illegible]	[illegible]		Distributed C2	Seamless access
Distributed Collaborative Planning Tools	[illegible] shore based	VTC, Chat		Video over IP	Shareable S[illegible]

FOR OFFICIAL USE ONLY

The Technical Cooperation Program

SUBCOMMITTEE ON NON-ATOMIC MILITARY RESEARCH AND DEVELOPMENT

TTCP TECHNICAL REPORT

FORCENET IMPLICATIONS FOR COALITIONS

OCTOBER 2007

TR-MAR-XX-2007

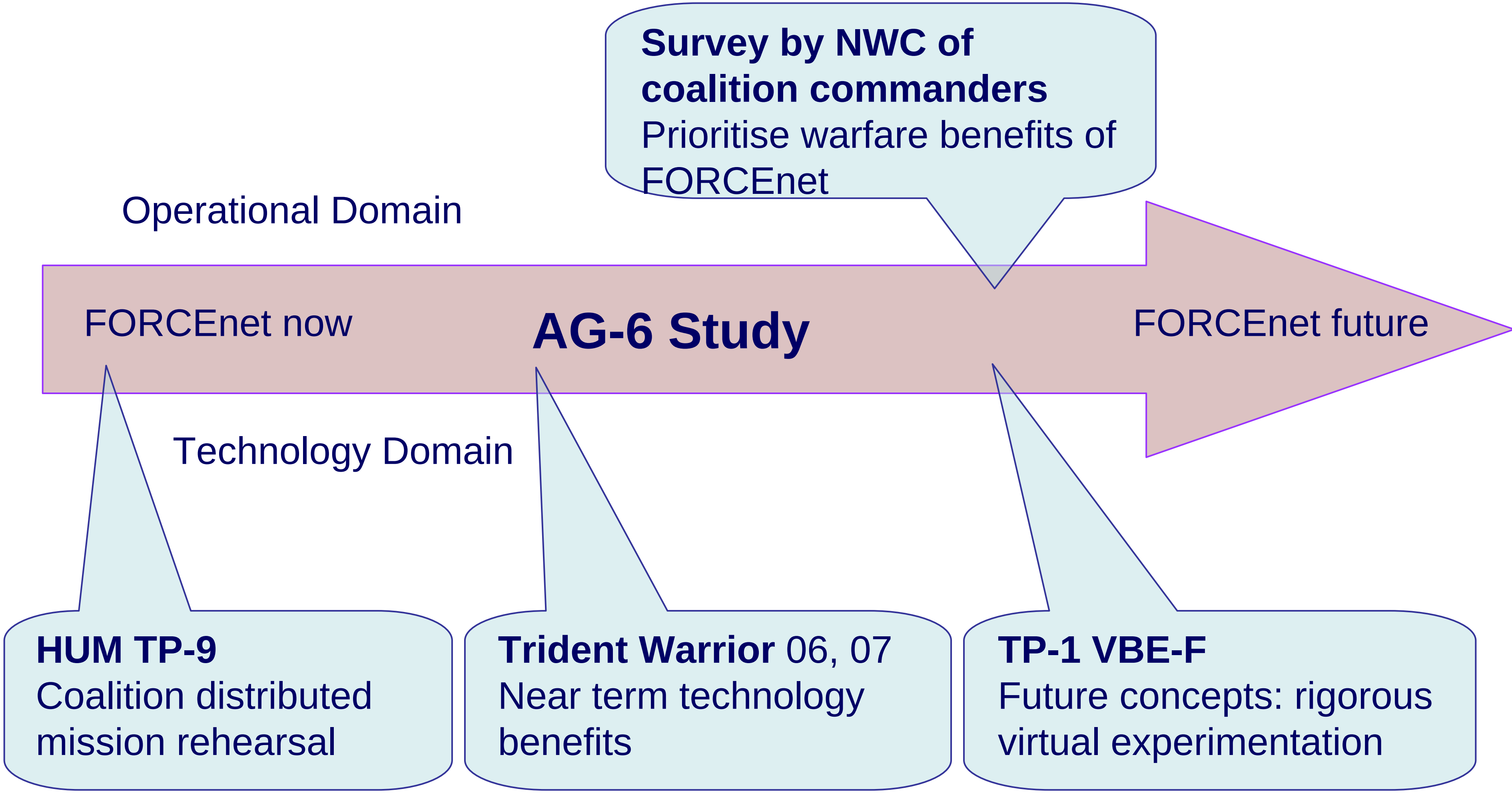
This document contains information that is provided in confidence to the Governments of Australia, Canada, New Zealand, the United Kingdom and the United States under The Technical Cooperation Program (TTCP) among these Governments. The information contained herein may be used and disseminated for national Defence Purposes Only within the recipient Governments and their national defence contractors. The recipient Governments will ensure that any other use or disclosure of the information is made only with the prior written consent of each of the above Governments.

FOR OFFICIAL USE ONLY

AG-6 Measures of Effectiveness

High Level MoE:	Contributing Elements and Notes:
MoE1 Mission Success	Mission Outcome - no loss of major units (HVU) and successful completion of vignette mission
MoE2 Risk	Minimise blue attrition - sum total of unit losses during vignette
MoE3 Economy of Effort	Cost, for fuel and munitions expended in vignette
MoE4 Time to Capability	Time to Capability - gives credit for increased speed of integration of force for mission implied in vignette Limits enemy's ability to generate his own forces.

Validation Alignment: Technology & Operations



Survey by NWC of coalition commanders
Prioritise warfare benefits of FORCEnet

Operational Domain

FORCEnet now

AG-6 Study

FORCEnet future

Technology Domain

HUM TP-9
Coalition distributed mission rehearsal

Trident Warrior 06, 07
Near term technology benefits

TP-1 VBE-F
Future concepts: rigorous virtual experimentation